НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.050903 Телекомунікації
(172 Телекомунікації та радіотехніка)

на тему: «Аналіз варіантів розвитку протоколу OLSR»

Виконала:
студентка IV курсу, групи ТС-51
Пивовар Дарина Михайлівна _____

Керівник:
Доцент кафедри ТС, к. т. н., доцент
Максимов В. В. _____

Рецензент:
Доцент кафедри ТК, к. т. н., с. н. с.
Тріска Н. Р. _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.
Студентка _____

Київ – 2019 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки– 6.050903 «Телекомунікації» (172 Телекомунікації та радіотехніка)

Програма професійного спрямування – «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту
Пивовар Дарині Михайлівні

1. Тема роботи «**Аналіз варіантів розвитку протоколу OLSR**», керівник роботи Максимов Володимир Васильович кандидат технічних наук, доцент, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом роботи 10 червня 2019 р.

3. Вихідні дані до роботи: RFS протоколу OLSR, AIS-OLSR.

4. Зміст роботи:

Розглянути протокол маршрутизації OLSR, визначити його переваги та недоліки. Дослідити алгоритм роботи цього протоколу, провести аналіз його модифікацій, визначити їх характеристики та можливі сфери використання даних протоколів.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): 1) Тема та мета дипломної роботи; 2) Протокол OLSR; 3) Модифікації протоколу OLSR: AIS-OLSR, QOS-OLSR, MP-OLSR; 4) SU-OLSR; 5) Висновки

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Аналіз отриманого завдання	04.09.18-17.09.18	
2.	Постановка мети дипломної роботи та розробка пунктів змісту	18.09.18-08.10.18	
3.	Формування вступної частини пояснювальної записки	09.10.18-31.10.18	
4.	Формування першого розділу пояснювальної записки	1.11.18-20.12.18	
5.	Формування другого розділу пояснювальної записки	21.12.18-18.02.19	
6.	Формування третього розділу пояснювальної записки	19.02.19-10.04.19	
7.	Оформлення дипломного проекту	11.04.19-01.05.19	
8.	Чистовий варіант дипломної роботи, плакати	02.05.19-20.05.19	

Студент Пивовар Д. М.

Керівник роботи Максимов В. В.

РЕФЕРАТ

Пояснювальна записка викладена на 79 сторінках та включає 24 ілюстрацій, 9 таблиць та 22 джерел за переліком посилань.

Метою роботи є аналіз модифікацій протоколу маршрутизації OLSR.

В даній роботі розглядається протокол маршрутизації OLSR, принцип та алгоритм його роботи. Визначаються переваги та недоліки цього протоколу. Проведений аналіз модифікацій протоколу OLSR, їх алгоритм роботи. Визначено способи усунення деякий недоліків основного протоколу за допомогою даних модифікацій.

Велику увагу приділяється модифікації SU-OLSR. Цей варіант розвитку основного протоколу виконує визначення підозрілих MPR. Визначено основні недоліки протоколу.

OLSR, MANET, AD-HOC, MPR, TC.

ABSTRACT

The theme of the work is "Analysis of the options for the development of the protocol OLSR".

The purpose of the work is to analyze the modifications of the protocol routing OLSR.

In this paper, OLSR routing protocol is considered, the principle and algorithm of its work. The advantages and disadvantages of this protocol are determined. An analysis of protocol modifications OLSR, their algorithm of work is carried out. The ways of eliminating some of the disadvantages of the main protocol with the help of these modifications are determined.

Much attention is paid to SU-OLSR modifications. This variant of the development of the main protocol performs the definition of suspicious MPR. The main shortcomings of the protocol are determined.

OLSR, MANET, AD-HOC, MPR, TC.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AIS	Artificial Immune System	Штучна імунна система
BER	Bit Error Rate	Частота помилок по бітам
CBR	Constant Bit Rate	Постійна бітова швидкість
DARPA	Defense Advanced Research Projects Agency	Агентство передових оборонних дослідницьких проектів
GloMo	Global Mobile Information Systems	Глобальні мобільні інформаційні системи
IEEE	Institute of Electrical and Electronics Engineers	Інститут інженерів з електротехніки та електроніки
IETF	Internet Engineering Task Force	Інженерний рада інтернету
INRIA	Institut National de Recherche en Informatique et Automatique	Національний інститут наукових інтересів та інформатики
LPR	Low-cost Packet Radio	Недорогий радіозв’язок
MANET	Mobile Ad-hoc Network	Мобільна Ad-hoc мережа
MP-OLSR	MultiPath Optimized Link State Routing protocol	Протокол маршрутизації багатоканального оптимізованого посилання
MPR	MultiPoint Relays	Мультиточкові реле
NS-2	Network Simulator 2	Симулятор мережі скорочень
NTDR	Near-term digital radio	Близьке цифрове радіо
OLSR	Optimized Link State Routing	Оптимізований протокол маршрутизації зв'язку
OLSRv1	OLSR version 1	OLSR версії 1
OLSRv2	OLSR version 2	OLSR версії 2
PDR	Packet Delivery Ratio	Коефіцієнт доставки пакетів
PRNet	Packets Radio Network	Пакети радіомережі

QoS-OLSR	Quality of Service extension introduced to the OLSR protocol	Розширення якості обслуговування введено в протокол OLSR
RFC	Request for Comments	Запит коментарів
SU-OLSR	Suspicious OLSR	Підозрілий в OLSR
SURAN	Suvivable Radio Networks	Придатні радіомережі
TC	Topology Control	Керування топологією

ВСТУП

Останнім часом інтерес дослідників викликають мережі MANET: багатокрокові бездротові мережі, що самоорганізовуються, з розподіленим управлінням, в яких передача даних між двома вузлами можлива через проміжні вузли. Топологія таких мереж може змінюватися з часом, тому для коректної роботи мережі необхідний механізм маршрутизації пакетів, який би автоматично збирав актуальну інформацію про топологію мережі і керував ретрансляцією пакетів від джерела до кінцевого одержувача. Це забезпечується за допомогою протоколу маршрутизації. Досить популярні мережі MANET, побудовані на базі стандарту IEEE 802.11, в яких в якості протоколу маршрутизації використовується Optimized Link State Routing (OLSR) [1].

Оптимізований протокол маршрутизації каналів зв'язку OLSR розроблений для мобільних спеціальних мереж. Він функціонує як проактивний протокол, керований таблицями, тобто регулярно обмінюється інформацією топології з іншими вузлами мережі. Кожен вузол вибирає набір своїх сусідніх вузлів як "багатоточкові реле" (MPR). В OLSR тільки вузли, обрані як такі MPR, відповідають за пересилання трафіку керування, призначеного для дифузії у всю мережу [2].

1 ПРОТОКОЛ OLSR

1.1 Історія розвитку Ad-hoc мережі

Спочатку розвиток Ad-hoc мереж був результатом вимоги військових до швидкого розгортання телекомунікаційних інфраструктур. Централізована мережа навколо базових станцій не є хорошим варіантом для такого середовища, оскільки вони повинні бути розгорнуті в першу чергу (практично неможливо у ворожій місцевості). Мережа стає вразливою, якщо одна або більше з цих станцій бази руйнуються.

У 1972 році Міністерство оборони США, зокрема агентство оборонних наукових проектів (DARPA), спонсорувало програму досліджень Packets Radio Network (PRNet) [3]. Цей проект стосувався, зокрема, проблеми маршрутизації та доступу до засобів масової інформації у мережі мультихопної радіохвилі.

У 1983 році цей проект перетворився на програму Suvivable Radio Networks (SURAN), яка стосувалася, зокрема, питань безпеки, енергоменеджменту та переробних потужностей [4]. Завдання полягали в тому, щоб збільшити кількість вузлів, що підтримуються PRNet в розширеній географічній області, і зменшити споживання енергії шляхом розробки нових алгоритмів маршрутизації. Low-Packet Radio (LPR) був результатом цього дослідження в 1987 році [5]. Технологія LPR запропонувала комутацію пакетів, покращення безпеки та управління споживанням енергії вузлами.

Ще в 1990 році ноутбуки оснащувалися бездротовими картами та інфрачервоними портами, що дозволяло безпосереднє та непряме спілкування між ноутбуками. Таким чином, технологія PRNet стала доступною для широкої громадськості за допомогою реальних цивільних заявок. Після цього IEEE ввів термін «Ad-Hoc Networks» для стандарту IEEE 802.11 для бездротових локальних мереж.

Завдяки важливості бездротових мереж у 1994 році, DARPA спонсорувала програми Global Mobile Information Systems (GloMo) та Near-term digital radio (NTDR). Метою цих програм було розробка бездротових мереж Ad-Hoc, які пропонували мультимедійне комунікаційне середовище в будь-який час і в будь-якому місці. NTDR все ще використовується армією США.

Ряд стандартів слідував за розвитком мереж Ad-Hoc. Так було створено робочу групу «Мобільна мережа Ad-Hoc Networks» (MANET) в рамках Internet Engineering Task Force (IETF). Метою цієї групи було спробувати стандартизувати протоколи маршрутизації в мережах Ad-Hoc. Кілька військових та цивільних застосувань згодом слідували за появою мереж Ad-hoc [1].

1.2 Принцип роботи OLSR

Протокол OLSR добре підходить для великих і щільних мобільних мереж, оскільки оптимізація, що досягається за допомогою MPR, добре працює в цьому контексті. Чим більша і щільніша мережа, тим більше оптимізації може бути досягнуто в порівнянні з класичним алгоритмом стану зв'язку. OLSR використовує маршрутизацію "хоп-по-хопу", тобто кожен вузол використовує свою локальну інформацію для маршрутизації пакетів.

OLSR добре підходить для мереж, де трафік є випадковим між більшим набором вузлів, а не між невеликим певним набором вузлів. В якості проактивного протоколу OLSR також підходить для ситуацій, коли пари комунікацій змінюються з часом: у цій ситуації не створюється додатковий трафік управління, оскільки маршрути підтримуються для всіх відомих напрямків у будь-який час [2].

OLSR відноситься до сімейства проактивних протоколів і розроблена для Ad-Hoc мереж. Цей протокол був розроблений в рамках проекту HIPERCOM в INRIA. OLSR була обрана групою IETF MANET для

стандартизації. Версія OLSR 1 була стандартизована з 2003 року і вказана в RFC3626 [1].

OLSR, найпопулярніший проактивний протокол маршрутизації для Ad-hoc мереж і OLSR версії 1 (OLSRv1), був стандартизований як експериментальний Request for Comments (RFC). Це протокол стану каналу, в якому кожен вузол періодично надсилає повідомлення HELLO і TC (топологічний контроль). Це зменшує накладні витрати на інформацію про стан затоплення, вимагаючи лише перенаправлення повідомлень TC на MPR. Таблиця маршрутизації підтримується для збереження наступної інформації про стрибок до всіх можливих вузлів призначення.

OLSR версії 2 (OLSRv2) має той же алгоритм і ідеї, що і OLSRv1. Будучи модульним за проектом, OLSRv2 складається з ряду узагальнених будівельних блоків, стандартизованих незалежно і застосовних також для інших протоколів MANET. Ця версія протоколу має більш модульну та розгалужену архітектуру, і є простішою та ефективнішою, ніж OLSRv1 [6].

Протокол OLSR є одним з найбільш популярних протоколів маршрутизації в мобільних багатокрокових бездротових мережах. Цей протокол вирішує завдання виявлення сусідніх вузлів і підтримки з'єднань з ними, поширення інформації про існуючі з'єднаннях з сусідніми вузлами по всій мережі, пошуку найкоротших маршрутів на підставі наявної на вузлі маршрутної інформації та покрокової ретрансляції пакетів.

Ad-Hoc мережі характеризуються динамічною та мінливою топологією. Для того, щоб виявити будь-які зміни в мережі та генерувати інформацію топології, протокол OLSR по суті базується на виявленні та оновленні списку сусідів кожного вузла. Надалі всі вузли мають один бездротовий інтерфейс.

Посилання між двома вузлами можна розділити на три категорії:

1. Асиметричне: посилання вважається несиметричним, якщо перший вузол отримав повідомлення від другого вузла, але не отримав підтвердження, що другий вузол це зрозумів.

2. Симетричне: посилання вважається симетричним, якщо кожен вузол чує інший.

3. Загублене: посилання вважається втраченим, якщо це посилання раніше було оголошено симетричним або асиметричним, але на даний момент повідомлення не отримано від вузла [1].

Для виявлення сусідніх вузлів і підтримки з'єднання з ними (пара вузлів є сусідами, якщо знаходяться в області впевненого прийому один одного) всі вузли мережі періодично (з інтервалом *HELLO_INTERVAL*) широкомовно розсилають службові повідомлення HELLO, що містять адреси сусідніх вузлів і інформацію про встановлені з ними з'єднаннях. Якщо протягом часу *NEIGHB_HOLD_INTERVAL* вузол не отримує жодного повідомлення HELLO від свого сусіда, то з'єднання з цим вузлом вважається розірваним. Повідомлення HELLO не ретранслюються по всій мережі, тому з їх допомогою кожен вузол може дізнатися мережеву інформацію лише про своє двокрокове оточення [2].

Назвемо вузол *n* однокроковим сусідом вузла *x* (або для стислості просто сусідом), якщо вузол *x* знаходиться в області впевненого прийому *n*. Вузол *d* який не є однокроковим сусідом вузла *x*, назвемо двокроковим сусідом вузла *x*, якщо вузол *d* є однокроковим сусідом хоча б одного однокрокового сусіда вузла *x*.

Для поширення інформації про з'єднання з однокроковими сусідами по всій мережі, вузли періодично (з інтервалом *TC_INTERVAL*) відправляють широкомовні повідомлення *TOPOLOGY_CONTROL* (ТС). Інформація про з'єднання між парою вузлів, отримана з ТС деякого вузла-джерела, оновлюється при отриманні кожного нового ТС повідомлення від цього вузла, і видаляється, якщо або вузол-джерело ТС більше не розсилає інформацію по даному з'єднанні, або завершився інтервал *TOP_HOLD_INTERVAL* з моменту отримання останнього ТС від розглянутого вузла джерела.

Всі широкомовні службові повідомлення ретранслюються з використанням випадкової затримки - джиттера; за замовчуванням він вибирається рівноймовірно їх інтервалу [0, HELLO_INTERVAL / 4).

На підставі інформації, отриманої з HELLO і TC, кожен вузол будує орієнтований граф, який є представленням бездротової мережі для даного вузла. До кожного вузла мережі в отриманому графі визначається найкоротший маршрут, що представляє собою ланцюжок ретрансляторів. Адреса кінцевого одержувача і першого ретранслятора утворюють запис в таблиці маршрутизації.

При необхідності доставити пакет до кінцевого одержувача вузол знаходить потрібний запис в таблиці маршрутизації і пересилає пакет вказаному в цій таблиці ретранслятору. Ретранслятор, отримавши пакет, проробляє аналогічну процедуру. При цьому маршрут, який використовується вузлом-ретранслятором, може відрізнятися від маршруту джерела, оскільки ретранслятор має власне бачення топології мережі. Таким чином, пакет передається до тих пір, поки не досягне кінцевого одержувача, чи не буде відкинутий в разі зациклення маршруту.

Ключовою особливістю протоколу OLSR, що знижує завантаженість мережі при широкомовній розсилці, є використання так званих MPR-ретрансляторів (MultiPoint Relays) (див Рис. 1.1).

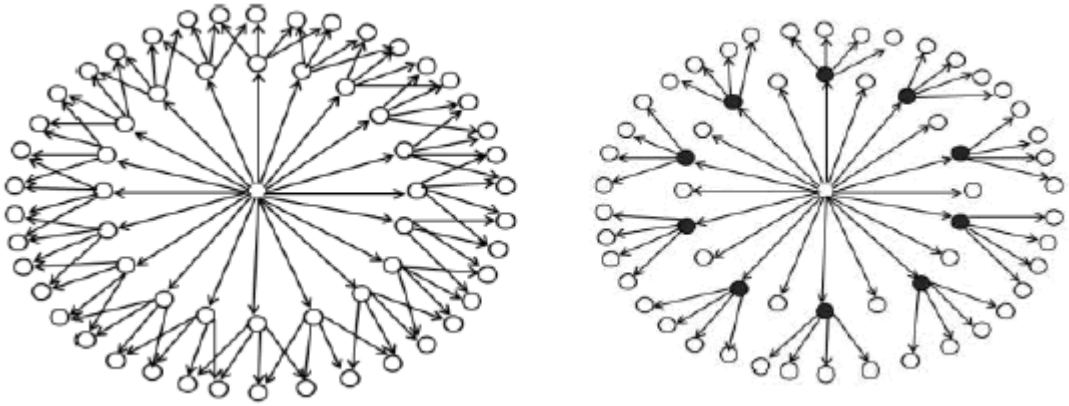

Рисунок 1.1 Вибір MPR

Кожен вузол вибирає з безлічі своїх однокрокових сусідів, з якими встановлено двонаправлене з'єднання, MPR-ретранслятори таким чином, щоб кожен двокроковий сусід даного вузла був однокроковим сусідом по крайній мірі одного з його MPR-ретрансляторів. MPR-ретранслятори грають важливу роль при поширенні маршрутної інформації та пересиланні широкомовних повідомлень. По-перше, кожен вузол, за замовчуванням, включає в повідомлення TC інформацію про двонапрямлені з'єднання тільки з тими сусідами, які вибрали даний вузол в якості MPR-ретранслятора. Завдяки цьому зменшується число з'єднань, інформація про які розсилається по мережі, як показано на Рис. 1.1. По-друге, вузол Y пересилає широкомовне повідомлення, отримане від його сусіда - вузла X, тільки в тому випадку, якщо Y є MPR-ретранслятором вузла X. Таким чином знижується число пересилань при поширенні одного широкомовного повідомлення [7].

1.3 Формат і генерація повідомлень HELLO

Спільний механізм використовується для заповнення локальної інформаційної бази зв'язку та інформаційної бази сусідства, а саме періодичного обміну повідомленнями HELLO.

Для пристосування для зондування зв'язку, виявлення сусідства та сигналізації вибору MPR, а також для врахування майбутніх розширень, застосовується підхід, подібний до загального формату пакетів.

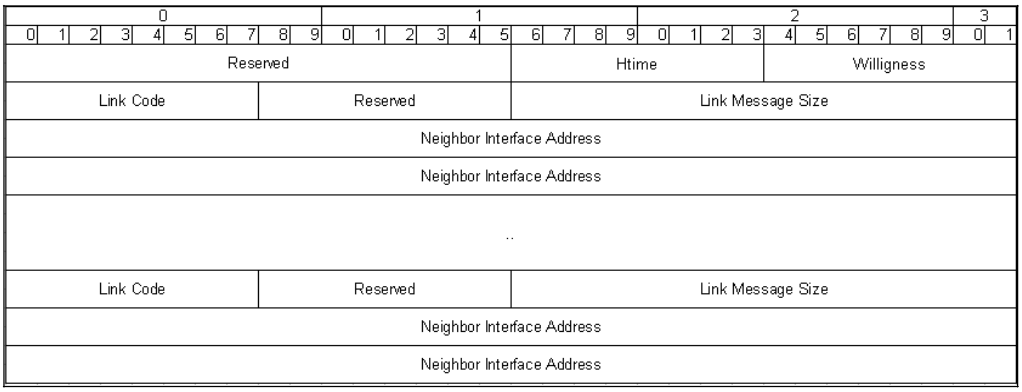

Рисунок. 1.2 Формат повідомлення HELLO

- Reserved (Зарезервований)

Це поле має бути встановлено на "0000000000000", щоб відповідати цій специфікації.

- HTime

Це поле визначає інтервал випромінювання HELLO, використовуваний вузлом на даному конкретному інтерфейсі, тобто час до передачі наступного HELLO. Інтервал випромінювання HELLO представлений його мантисою (чотири найвищих біта Htime-поля) та її експонентом (чотири найменших біта Htime-поля). Іншими словами:

Інтервал випромінювання:

$$HELLO = C*(1+a/16)*2^b \text{ [в секундах]} \quad (1.1)$$

де a є цілим числом, представленим чотирма високими бітами поля Htime,

b цілим числом, представленим чотирма найменшими бітами поля Htime. C = 1/16 секунд (дорівнює 0,0625 секунд).

- Willingness (Готовність)

Це поле вказує на готовність вузла переносити і пересилати трафік для інших вузлів.

WILL_NEVER = 0

WILL_LOW = 1

WILL_DEFAULT = 3

WILL_HIGH = 6

WILL_ALWAYS = 7

Готовність вузла може бути встановлена на будь-яке ціле значення від 0 до 7 і визначає, наскільки бажано вузлу пересилати трафік від імені інших вузлів. Вузли за замовчуванням матимуть бажання WILL_DEFAULT. WILL_NEVER вказує на вузол, який не бажає переносити трафік для інших вузлів, наприклад, через обмеження ресурсів (наприклад, низький рівень

заряду акумулятора). WILL_ALWAYS вказує, що вузол завжди повинен бути обраний для перенесення трафіку від імені інших вузлів, наприклад, через достаток ресурсів (наприклад, постійний блок живлення, інтерфейси високої ємності з іншими вузлами).

Вузол може динамічно змінювати свою готовність при зміні його умов.

Вузол з готовністю WILL_NEVER ніколи не повинен вибиратися як MPR будь-яким вузлом. Вузол з готовністю WILL_ALWAYS повинен завжди вибиратися як MPR.

- Link Code (Код посилання)

Це поле вказує інформацію про зв'язок між інтерфейсом відправника та наступним списком сусідніх інтерфейсів. Він також вказує інформацію про статус сусіда.

Коди посилань, не відомі вузлу - відкидаються.

- Link Message Size (Розмір повідомлення посилань)

Розмір повідомлення зв'язку, розрахований в байтах і виміряний від початку поля "Код посилання" і до наступного поля "Код посилання" (або - якщо немає більше типів посилань - кінець повідомлення).

- Neighbor Interface Address (Адреса інтерфейсу сусідства)

Адреса інтерфейсу сусіднього вузла [2].

1.4 Формат повідомлення TC

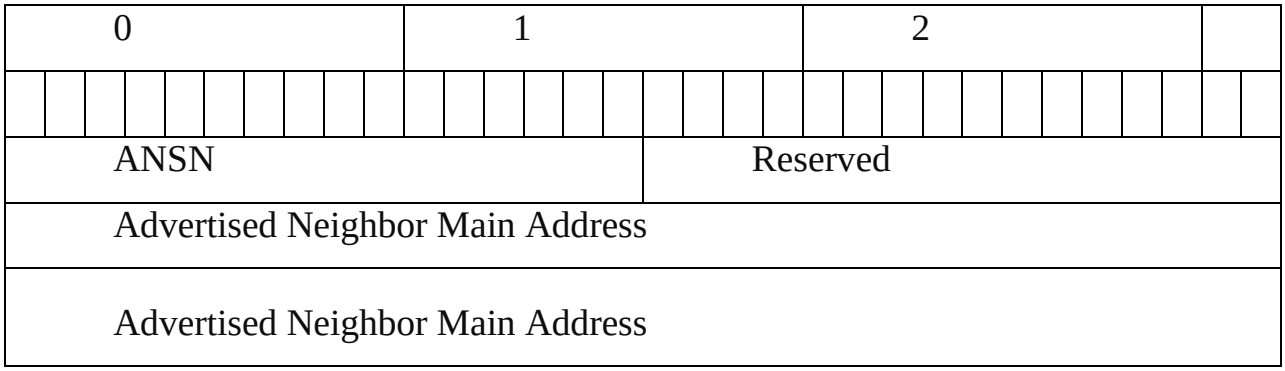

Рисунок 1.3 Формат повідомлення TC

- ANSN (Номер послідовності оголошених сусідів)

Порядковий номер пов'язаний з набором оголошених сусідів. Кожен раз, коли вузол виявляє зміну в своєму оголошеному наборі сусідів, він збільшує цей порядковий номер. Цей номер надсилається в цьому полі ANSN повідомлення TC для відстеження останньої інформації. Коли вузол приймає повідомлення TC, він може прийняти рішення на основі цього номера послідовності оголошення.

- Advertised Neighbor Main Address (Основна адреса рекламованих сусідів)

Це поле містить основну адресу сусіднього вузла. Всі основні адреси оголошених сусідів вузла-джерела розміщуються в повідомленні TC. Якщо максимально дозволений розмір повідомлення (встановлено мережею) досягається, коли ще є оголошені адреси сусідів, які не були вставлені в TC-повідомлення, будуть генеруватися більше TC-повідомлень, поки не буде відправлено весь рекламований набір сусідів. Додаткові головні адреси сусідніх вузлів можуть бути включені, якщо бажано надмірність.

- Reserved (Зарезервований)

Це поле зарезервоване і повинне встановлювати значення "0000000000000000".

Для того, щоб побудувати топологічну інформаційну базу, кожен вузол, який був обраний як MPR, транслює повідомлення Topology Control (TC). TC-повідомлення підключені до всіх вузлів мережі і використовують переваги MPR. MPR дозволяють краще масштабувати при розподілі топологічної інформації [8].

Список адрес може бути частковим у кожному TC-повідомленні (наприклад, через обмеження розміру повідомлення, накладених мережею), але синтаксичний аналіз всіх TC-повідомлень, що описують оголошений набір посилань вузла, ПОВИНЕН бути завершеним протягом певного

періоду оновлення (TC_INTERVAL)). Інформація, рознесена в мережі цими TC-повідомленнями, допоможе кожному вузлу обчислити його таблицю маршрутизації.

Коли набір посилань вузла стає порожнім, цей вузол повинен продовжувати надсилати (порожні) TC-повідомлення протягом тривалості, рівної "часу дії" (як правило, це буде дорівнює TOP_HOLD_TIME) попередньо випущених TC-повідомлень, щоб анулювати попередні повідомлення TC. Потім він повинен припинити надсилання TC-повідомлень, поки деякий вузол не буде вставлений у свій оголошений набір посилань.

1.5 Переваги протоколу OLSR

OLSR є проактивним протоколом маршрутизації для мобільних Ad-hoc мереж. Протокол успадковує стабільність алгоритму стану каналу і має перевагу: маршрути доступні відразу ж коли це необхідно через його проактивний характер. OLSR - це оптимізація по протоколу стану класичного зв'язку, призначена для мобільних мереж Ad-hoc. OLSR мінімізує накладні витрати від переповнювання керуючого трафіку, використовуючи тільки вибрані вузли, так звані MPR, для повторної передачі керуючих повідомлень.

Цей метод значно скорочує кількість повторних передач, необхідних для доведення повідомлення всім вузлам мережі. По-друге, OLSR вимагає, щоб тільки частково посилання було затоплено, щоб забезпечити найкоротші шляхи маршруту. Мінімальний набір необхідної інформації про стан лінії зв'язку полягає в тому, що всі вузли, вибрані як MPR, ПОВИННІ оголошувати посилання на їх селектори MPR. Додаткова топологічна інформація, якщо вона присутня, МОЖЕ використовуватися, наприклад, для цілей надмірності.

OLSR може оптимізувати реактивність до топологічних змін за рахунок скорочення максимального інтервалу часу для періодичної передачі

керуючих повідомлень. Крім того, оскільки OLSR постійно підтримує маршрути для всіх пунктів призначення в мережі, протокол корисний для шаблонів трафіку, де велика кількість вузлів зв'язується з іншою великою підмножиною вузлів і де пари (джерело, одержувач) змінюються з часом. Протокол особливо підходить для великих і щільних мереж, оскільки оптимізація, виконана з використанням MPR, добре працює в цьому контексті. Чим більше і щільніше мережа, тим більше оптимізація може бути досягнута в порівнянні з класичним алгоритмом стану посилання.

OLSR призначений для роботи повністю розподіленим чином і не залежить від будь-якого центрального об'єкта. Крім того, OLSR не вимагає послідовної доставки повідомлень. Кожне керуюче повідомлення містить порядковий номер, який збільшується для кожного повідомлення. Таким чином, одержувач контрольного повідомлення може, при необхідності, легко ідентифікувати, яка інформація пізніша, навіть якщо повідомлення були переупорядкувані під час передачі.

OLSR не вимагає яких-небудь змін в форматі IP-пакетів. Таким чином, будь-який існуючий IP-стек може використовуватися як є: протокол взаємодіє тільки з керуванням таблиці маршрутизації.

1.6 Недоліки протоколу OLSR

Мобільна Ad-hoc мережа (MANET) - це самоорганізований набір мобільних вузлів. Повідомлення в MANET здійснюється за допомогою бездротового носія. Спеціальні бездротові мережі мають величезний комерційний та військовий потенціал через підтримку мобільності. Через складні мультимедійні програми в режимі реального часу, підтримка якості послуг у такій інфраструктурі стала важливою. Радіоперешкоди та ресурси низької ємності в спеціальних бездротових мережах ускладнюють якість обслуговування. Від'єднання MPR є головною проблемою в MANET, завдяки частій зміні топології мережі. Отже, ефективність протоколу маршрутизації

буде послаблено, оскільки це негативно впливає на рівень підключення мережі.

Протокол не забезпечує надійну передачу керуючих повідомлень: кожен вузол періодично відправляє керуючі повідомлення і тому може підтримувати розумну втрату деяких таких повідомлень. Такі втрати часто виникають в радіомережах через зіткнення або інших проблем з передачею.

OLSR демонструє гарні результати у великих та складних мережах, маленьку затримку при з`єднанні, але неефективно витрачає енергію неактивних пристроїв.

Також, в порівнянні, з іншими протоколами у OLSR: більші витрати інформації при передаванні та доставці; більша степінь займання трафіку маршрутною інформацією, через це займає більше часу для передавання інформації та довгий маршрут.

OLSR страждає на ще одну серйозну проблему. Цей протокол не розглядає такі параметри, як енергетичний рівень вузлів та довжину зв'язків у обробці маршруту.

Не має можливості для вузлів OLSR (без можливостей багатоадресної передачі) приєднуватися до груп багатоадресної передачі та отримувати багатоадресну передачу даних.

Оригінальний OLSR страждає низькою пропускною здатністю та пропускною спроможністю.

Кожен MPR у цьому протоколі повинен транслювати топологічну інформацію та пересилати повідомлення до цільових вузлів. Якщо один з цих MPR є зловмисним, це стане небезпекою для безпеки всієї мережі. На жаль, протокол OLSR не використовує поняття «довіри між вузлами». Тому можуть бути атаки містифікації посилань, коли шкідливий вузол намагається змусити своїх сусідів вибирати його як MPR.

1.7 Висновки з розділу 1

Отже, в даному розділі розглянуто історію виникнення Ad-Hoc мереж. Досліджено роботу проактивного протоколу маршрутизації OLSR, виділено його переваги та недоліки. Основна функціональність OLSR визначає поведінку вузла, оснащеного інтерфейсами OLSR, що беруть участь в MANET і виконують OLSR як протокол маршрутизації. Це включає в себе універсальну специфікацію повідомлень протоколу OLSR і їх передачу по мережі, а також визначення зв'язку, топологічну дифузію і розрахунок маршруту.

2 МОДИФІКАЦІЇ ПРОТОКОЛУ OLSR

Останні розробки в області бездротових мереж призводять до розвитку короткоживучих мереж MANET. Протоколи маршрутизації в MANET класифікуються за трьома категоріями. протоколи, керовані таблицями, за запитом і гібридні протоколи. OLSR є одним з прикладів протоколу маршрутизації, керованого таблицями, який найкраще підходить для щільних мереж, які спрямовані на зменшення накладних витрат на маршрутизацію. Він використовує маршрутизацію стану зв'язку як свою базу, а мінімальний підрахунок хопу - метрику для пошуку найкоротших шляхів. Але в щільних мережах може існувати кількість різних шляхів для досягнення призначення з різними метриками витрат, тому деякі обмеження якості обслуговування можуть допомогти вибрати кращий маршрут до місця призначення. Основний протокол OLSR має певні недоліки, такі як кількість повторних передач, нестабільність маршруту, втрати пакетів, затримка тощо.

В даному розділі розглядаються опис модифікацій протоколу OLSR. Такі модифікації допомагають вирішити деякі проблеми основного протоколу, такі як: циклічне перемикання, перенавантаження, затримка, нестабільність набору MPR, захист від атак на інформацію, що передається між вузлами, велика кількість повторних передач, затрата великої кількості енергії при передаванні, велика відстань, яку потрібно подолати інформації щоб дійти до кінцевого пункту.

2.1 AIS-OLSR

OLSR страждає на серйозну проблему. Цей протокол не розглядає такі параметри, як енергетичний рівень вузлів та довжину зв'язків у обробці маршруту. Штучна імунна система (AIS) використовується для підвищення ефективності протоколу маршрутизації OLSR. Запропонований алгоритм, що

називається AIS-OLSR [9], враховує кількість переходів, залишкову енергію в проміжних вузлах та відстань між вузлами, яка реалізується за допомогою негативного відбору та алгоритмів ClonalG AIS.

Серед параметрів при виборі відповідного маршруту, можна назвати три найбільш важливих:

1) вибір маршруту;
2) енергію що залишилася в проміжних вузлах;
3) відстань між вузлами.

Рахунок сегментів обернено пропорційний значенню маршруту; чим вище кількість переходів, тим імовірніше, що маршрут не підходить. Частина, енергії що залишилася в проміжних вузлах безпосередньо пов'язана з величиною маршруту.

Чим вище енергія маршруту, тим краще пройти цей маршрут. Як тільки енергія проміжних вузлів буде використана, маршрут буде скинутий і передача буде перервана. Крім того, вибір маршрутів з більш високим енергоспоживанням призводить до уніфікованого розподілу енергоспоживання в мобільних вузлах Ad-hoc, що є критичною проблемою в мобільних мережах Ad-hoc.

Третій параметр - це відстань між вузлами джерела і одержувача в мобільних мережах Ad-hoc, що сприяє пошуку найкоротшого маршруту з точки зору довжини між двома джерелами і вузлами призначення через процес маршрутизації. Як згадувалося раніше при виконанні протоколу OLSR, щоб виявити своїх сусідів, вузли спочатку передають повідомлення HELLO сусідам, зберігають доставлену інформацію в таблиці і розподіляють повідомлення TC в мережі з використанням точок MPR. Таким чином, всі вузли мережі знають про існуючі з'єднання і деталі підключення до кожного вузла. Відповідна інформація зберігається в таблиці для кожного вузла.

1. Склад AIS-OLSR

Як уже згадувалося раніше, велика кількість алгоритмів призначена для штучних імунних систем, кожна з яких застосовується в різних областях. Застосований алгоритми негативного відбору і Clonal G.

2. Використання алгоритму негативного вибору

Алгоритм негативного вибору створюється на основі Т-клітин. Т-клітини розрізняють клітини інсайдера і аутсайдера. Він складається з двох етапів: перший, який є етапом навчання, подібний до спільної роботи і закінчується; це відноситься до комірок, які ідентифікують і видаляють інсайдерів. Потім другий етап, який є стадією тестування або реалізації, порівнює антигени з іншими Т-клітинами першої стадії і видаляє, якщо вони ідентифікуються. Основною функцією цього алгоритму є ідентифікація шаблону.

У зв'язку з цим ці алгоритми використовуються для створення набору антитіл, які обирають оптимальний маршрут серед них наступним чином:

Algorithm : Negative Selection Algorithm
1: **Input:** A S ⊂ U ("self-set"); a set M ⊂ U ("monitor set"); an integer n 2: **Output:** For each element m ∈ M, either "self" or "non-self"
3: **Procedure** Training phase 4: { 5: **d ← empty set** 6: while |D|< n do 7: **d ← random detector** 8: }

Рисунок 2.1 Алгоритм для створення набору антитіл

Вихідний вузол в стандартному OLSR, переглядаючи свою таблицю маршрутизації і маршрути до місця призначення, вибирає маршрут з мінімальною кількістю хостів, використовуючи алгоритм Дейкстра. Проте, процес, виглядає наступним чином: вихідний вузол вибирає маршрути з таблиці маршрутизації, яка веде до пункту призначення, але для вибору оптимального маршруту, по-перше, він застосовує алгоритм негативного вибору. У цьому алгоритмі антитіла є маршрутами, що досягають місця призначення в таблиці маршрутизації, тоді як антиген є механізмом, який перевіряє дві умови, включаючи кількість енергії і кількість ходів маршрутів. Кожен раз, через стадію сегрегації, одне антитіло (маршрут) порівнюють з одним антигеном до порівняння всіх антитіл. Потім відхиляються гірші маршрути з точки зору кількості використання енергії і кількості стрибків. При порівнянні антигену з антитілами (маршрутами), які відкидаються або зберігаються, кожне антитіло (маршрут) порівнюють з антигеном. Якщо вміст антитіл (маршруту) менше, ніж порогова енергія проміжних вузлів, воно відхиляється; в іншому випадку він вводиться в масив, аналізований з точки зору кількості переходів.

Цей поріг розраховується за формулою :

$$\frac{\text{Енергія вузла } i}{\text{Максимальна енергія вузлів}}, \qquad (2.1.)$$

де *i* - проміжні вузли кожного маршруту.

Кількість масивів визначається виходячи з кількості антитіл (маршрутів), призначених для групи. Кожен маршрут, що проходить через попередній етап, надходить в масив, і масив розміщується на основі повного переходу до адресата.

Потім, ввівши наступний маршрут, він порівнюється з масивом. Якщо кількість переходів маршруту більше, ніж маршрутів в масиві, він буде відхилений. Якщо не видалити такий маршрут, то він може замінити маршрут з максимальною кількістю переходів (і такий маршрут буде відхилений з масиву), і масив буде перегрупований. Цей процес виконується

до тих пір, поки всі маршрути не будуть протестовані, а ті що залишилися в масиві не ввійдуть в набір виявлення. Тому, згідно з алгоритмом негативного відбору, якщо дане антитіло (маршрут) відповідає умовам (енергія проміжного вузла низька, а кількість стрибків велика), маршрут буде відхилений; в іншому випадку він відкладається до наступного. Кращі маршрути відокремлюються від гірших, і кращі вибираються як члени набору виявлення.

Algorithm 1: Pseudo-code comparing Antigen with Antibody
1: **Input:** Antigen (Route's) 2: **Output:** Array of Routes

3: **Procedure** Comparing Antigen with Antibody
4: {
5: **If** energy(node i) < Threshold then 6: {
7: Delete (Route i)
8: **Else if**
9: {
10: Array ← Route i
11: Array Sort Order by hop count 12: }
13: }
14: **If** hop count (Route i) < hop count (Array Route) then 15: {
16: Delete (Route i)
17: **Else if**
18: Max (hop count) ← Route
19: }
20: }

Рисунок 2.2 Псевдокод, що порівнює Antigen з антитілом

На наступному етапі необхідно виконати дві інших дії:

1) при необхідності виконується гіпер-мутація;

2) краще антитіло (оптимальний маршрут) вибирається і зберігається в імунній пам'яті, що робиться з використанням алгоритму Clonal G.

3. Використання алгоритму ClonalG

Алгоритм CLONALG, враховуючи його критичну властивість, оптимізацію, підходить найкраще для цієї галузі. Алгоритм створює ранні комірки і виділяє колонку на кожен антиген. Потім отримані антитіла будуть використовуватися в якості вихідних елементів пам'яті на наступній ітерації; процес продовжується до виконання кінцевої умови. Таким чином, комірки пам'яті на кожній ітерації можуть бути створені з більш високою спорідненістю. Спорідненість відіграє важливу роль в колонізації комірок. Насправді, більш висока спорідненість викликає велику проліферацію, а більш низька спорідненість призведе до меншої проліферації.

Таблиця. 2.1 Відповідність між імунною системою і CLONAL-G

Імунна система	CLONAL-G
Антиген	Кращі маршрути з точки зору енергії та кроків
Антитіла	Вивчення енергії та умов кроку
Індекс спорідненості	Пропорція загальної енергії маршруту вузлів на енергію на переходах
Мутація	Порівняння маршрутів у відстані

4. Спорідненість

Різні дослідження вказують рівень зв'язування антигену і антитіла як на відстань, так і на спорідненість [10]. У цьому дослідженні вимірюється спорідненість по відношенню до загальної сумарної енергії вузлів маршруту до кроків всіх маршрутів спорідненості; потім вибирає маршрути з найвищою спорідненістю. Тому маршрути з найвищою спорідненістю будуть обрані і залишаться на наступних етапах, а інші маршрути будуть видалені.

5. Мутація і колонізація

Як тільки алгоритм ідентифікує маршрути з більш високою спорідненістю, при необхідності буде ініційована мутація. Швидкість мутації залежить від близькості, що означає, що якщо спорідненість велика, мутації не відбувається, а пам'ять безпеки зберігає маршрут, так що вихідний вузол вибирає цей маршрут при відправці пакетів в пункт призначення. З іншого боку, велика близькість маршрутів викликає мутацію. Фактично, маршрути спочатку впорядковуються на основі самої високої спорідненості в наборі; далі, N-номер цього набору з більш високою спорідненістю буде обраний для мутації. Мутація тут порівнює маршрути в відстані, і вибирає маршрут з найменшою відстанню між джерелом і пунктом призначення. Маршрут буде вибрано з поміж інших на останньому етапі. Кращий маршрут - найпотужніший і найменший. Цей оптимізований маршрут розміщується в пам'яті, який буде представлений як кращий маршрут для передачі даних (рис. 2.3). Показник протоколу AIS-OLSR для протоколу OLSR і EAOLSR, який є покращеною версією протоколу OLSR з точки зору енергетичного рівня, представлений з використанням швидкості доставки пакетів, затримки на кінець транзакції, пропускної здатності мережі і терміну служби мережі.

```
For all Routes Calculate :
Affinity= (Energy Route Nodes) / (hopcount)
If Affinity (Route i) > Max Affinity then
Self-Memory ←   Route i
Else
{
Mutation
For j=1 to N do
{
Distance (Route j)
Self-Memory ←   Minimum (Route j)
}
   }
```

Рисунок 2.3 Псевдокод мутація і колонізація

Як було сказано раніше, базовий протокол OLSR працює з найкоротшим числом переходів і використовує алгоритм Дейкстра для

маршрутизації. Передбачається, що всі вузли оснащені системою географічного позиціонування (GPS), завжди знаючи свої координати. Використовуючи запропонований метод в алгоритмі OLSR, в пакет повідомлень HELLO додаються три нових поля, включаючи «географічне положення», «відстань» і «енергія». Тут поле географічного положення використовується для вимірювання відстані між вузлами, в той час як поле відстані використовується для передачі відстані між вузлами в будь-якому переході до проміжного вузла. Нарешті, енергетичне поле вказує кількість енергії, що залишилася.

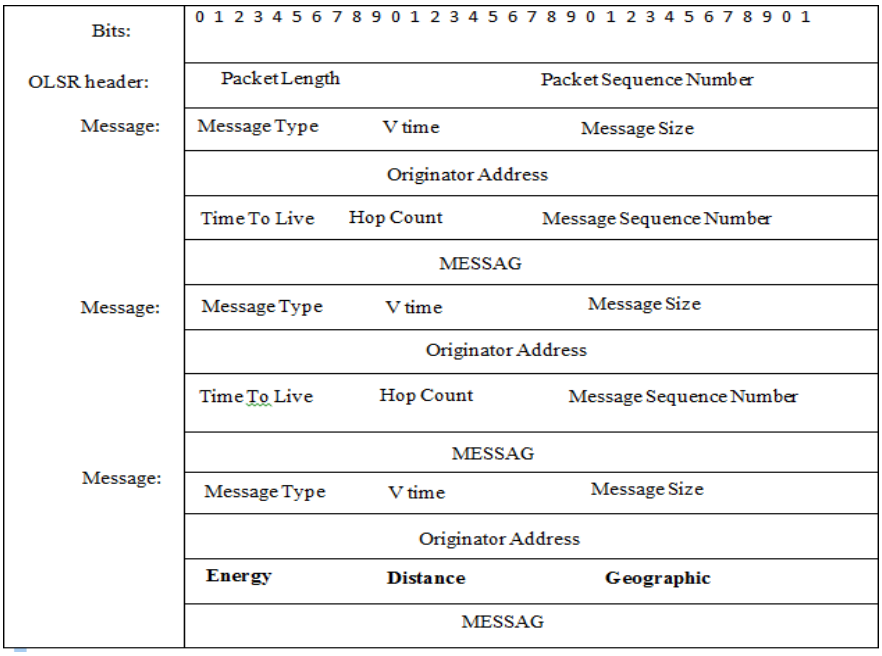

Рисунок 2.4 Псевдокод мутація і колонізація

Кожен вузол, який починає передавати повідомлення HELLO, спочатку ставить нульове значення в поле відстані, довготи і широти в поле географічного позиціонування, а його значення вмісту енергії в енергетичному полі потім вирушає в сусідні вузли. На підставі отриманих значень довготи і широти вузол, що приймає повідомлення, в свою чергу, обчислює відстань, використовуючи рівняння 2 і підсумовує його до значення в поле відстані і утримує його в таблиці як відстань. Потім він передає це значення, його географічне положення і його енергетичний вміст

у відповідь на повідомлення HELLO з ретрансляцією вузлів. Тому після поширення повідомлення HELLO всі вузли мають таблицю, в якій виявляються всі їхні сусіди; ідентифікуючи їх відстань до сусіднього вузла і енергетичний вміст сусідніх вузлів:

$$D = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}, \quad (2.2)$$

де, (x1, y1) і (x2, y2) - вказані географічні положення вузла, який повідомляє повідомлення HELLO

D - відстань між вихідним і кінцевим вузлами і сусіднім вузлом відповідно

Потім кожен вузол відправляє свою власну інформацію та зібрану інформацію про сусідів у вигляді повідомлення TC, що включає в себе три значення відстані, довготи і широти, а також енергетичні поля, з підрахунком переходів і числовими полями (які знаходяться в основному кадрі протоколу) MPR, через які повідомлення TC розповсюджуються в мережі. Як тільки повідомлення TC будуть розподілені, всі вузли мережі матимуть таблицю, що складається з усієї інформації вузлів, використовуваної в процесі маршрутизації. У стандартному протоколі OLSR для маршрутизації використовується тільки критерій підрахунку точок. Однак в цьому методі, в штучної імунної системи також враховуються два інших критерія, включаючи енергію і відстань [9].

2.2 QoS-OLSR

Quality of service (QoS) - це термін, широко використовуваний в останні роки в області дротових мереж, контрольованих централізованою адміністрацією, де присутня фіксована інфраструктура. Однак проблема для маршрутизації QoS в бездротовому середовищі через динамічний характер вузла та мобільність. Провайдери надають протоколи QoS з урахуванням деяких конкретних сценаріїв та з урахуванням різних параметрів зв'язку

(затримки, пропускної здатності, ймовірності втрати та рівня помилки), топологій мережі та змінних [11].

Для того, щоб отримати QoS, основний акцент повинен бути на отримання найкращої пропускної здатності та мінімальної швидкості пропуску. Проте мережам важко відрізнити різні типи контрольних повідомлень. Метрика пропускної здатності використовується для визначення суми пропускної здатності, яка буде доступна вздовж шляху від ініціатора до пункту призначення. Є критерії вибору вузла MPR на основі найкращого тракту пропускної здатності. Хоча це, здається, оптимальне рішення, але існують такі фактори, як втручання та радіоперешкоди в мережі, де, незважаючи на наявність більшої доступної пропускної здатності, відбувається несподівана затримка. Можна зосередиди увагу на механізмі контролю доступу, так що розрахунок пропускної здатності виконується під час розрахунку таблиці маршрутизації. Але тут невикористана пропускна здатність розраховується з урахуванням смуги пропускання, що споживається по посиланню іншими вузлами.

Протокол OLSR може бути налаштований, і можна побачити, що продуктивність в OLSR змінюється, а ефективність залежить від залишкової енергії вузлів. Існують різні методи відбору MPR та алгоритми визначення шляху. У модифікованій маршрутизації оригінальні критерії вибору MPR об'єднуються з новим алгоритмом визначення шляху. І в іншому варіанті Модифікований MPR / Маршрутизація нового вибору MPR та алгоритм визначення нового шляху об'єднуються.

Ці зміни значною мірою впливають на ефективність OLSR. Також протокол може бути змінений на основі "Скільки існує інформація про залишкову енергію". Залишкова енергія в той час, коли вибрано MPR, є ідеальною версією. У реалістичній версії дані про залишкову енергію, зібрані за протоколом обміну повідомленнями. Також змінюється топологічний вплив кількості доставлених пакетів та точності залишкового рівня енергії. Пакет латентний також впливає на точність зібраних даних.

На Рис 2.5, наведеній нижче, порівнюється продуктивність ідеальної та фактичної версії OLSR при різних трафіках. Здійснюється порівняння ефективності мережі в термінах доставлених пакетів у зв'язку зі зміною часу інтервалу пакетів. Оскільки час інтервалу пакетів зменшується (X-вісь), доставляється більше кількість пакетів, а також більше неналежної інформації про залишкову енергію збирають вузли в MANET. Отже, неточність менше і продуктивність системи збільшується. Це вірно як у ідеалі, так і в реалістичному підході, оскільки час інтервалу пакетів знижує ефективність. Але коли порівнюється ідеал з реалістичним, ідеальний перевершує реалістичний для кожного шматка даних. Це означає, що достатньо збирати інформацію про залишкову енергію у той час, коли обрано MPR.

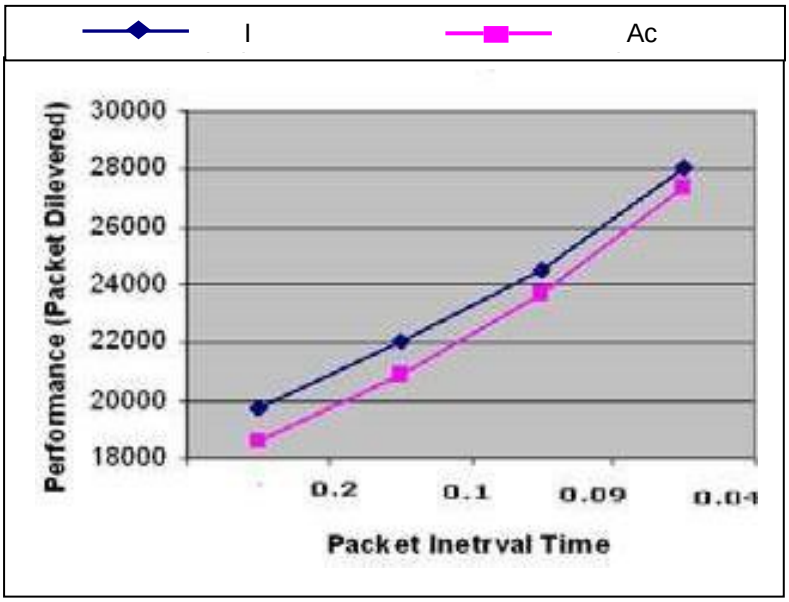

Рисунок 2.5 Ідеальна та фактична продуктивність

В енергоефективних варіаціях OLSR MPR вибираються на основі залишкових енергетичних рівнів вузлів. Алгоритм визначення шляху змінюється, вибираючи шляхи на основі залишкового рівня енергії проміжних вузлів. Уникати вузлів з низькою залишковою енергією. Вибір маршруту та MPR такий, щоб максимізувати рівень залишкової енергії у

вузькому місці. Це підвищить ефективність роботи мережі. Якщо неправильна або стара інформація збирається вузлами, то ефективність знижується, оскільки маршрут може зникнути. Але головне питання полягає в тому, як зібрати правильну інформацію про залишкову енергію.

Одним із рішень є використання EOLSR [11], що вибирають маршрут і MPR на основі залишкової енергії вузлів та кількості сусідів. Ідеальний підхід - надсилання більшої кількості пакетів, ніж реалістичний підхід, наведений вище. Оскільки швидкість руху зростає від низької до високої, при ідеальному підході надсилається все більше пакетів. Знаючи енергетичний рівень вузла можна забезпечити надсилання більше пакетів, ніж при реалістичній версії. Оскільки вибір дуже маленьких значень для інтервалів Hello і TC значно збільшить накладні витрати на протокол. Настільки реалістичний підхід з зменшенням часу інтервалу пакетів все більше і більше повідомлень TC та Hello надходять в мережу, що збільшує накладні витрати мережі. Ось чому реалістичний підхід є менш ефективним, ніж ідеальний, як показано на Рис. 2.5. Ці результати є прямим наслідком збільшення рівня заторів в мережі, що призводить до високої втрати повідомлень та затримки, а отже, менш точної інформації про стан. На Рис. 2.6 порівнюється OLSR та EOLSR, і це чітко видно, як енергія змінюється залежно від мережевого життя. З часом енергія вузлів розпадається дуже швидко. У OLSR MPR не часто змінюються, а ефективність знижується. Проте, у EOLSR вибір MPR залежить від залишкового рівня енергії з вузлів. Таким чином, EOLSR показує себе краще, ніж OLSR.

Це дослідження показує, що вузли мають неточні дані про фактичні залишкові рівні енергії при прийнятті рішень маршрутизації. Модифікація параметрів протоколу OLSR (наприклад, збільшення швидкості повідомлень Hello або TC) має дуже обмежений вплив на цю неточності.

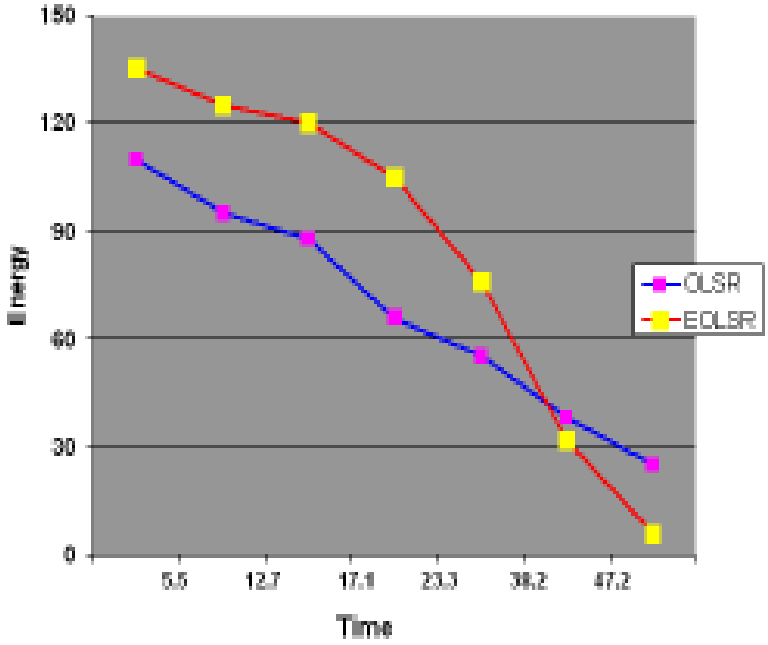

Рисунок 2.6 Рівні залишкової енергії OLSR та EOLSR

Це означає, що, збільшуючи частоту повідомлень TC та Hello, миттєво покращуємо інформацію про залишкову енергію сусідніх вузлів, але збільшуємо витрати на трафік. Тому для підвищення точності інформації про стан енергії потрібен інший спосіб.

Тому запропоновано метод прогнозування для підвищення точності рівня енергії, що перевищує та змінює параметри протоколу. Ясно видно, що збільшення частоти пакетів не покращує неточну енергетичну інформацію. Отже, для обчислення залишкової енергетичної інформації вузлів потрібна інша техніка. Тому пропонується, що механізм прогнозування обчислює залишкову енергетичну інформацію, яка є більш точною, ніж попередній метод. Ідея полягає в тому, щоб кожен вузол локально коригував старі енергетичні рівні вузлів на основі їх минулого споживання енергії. У цьому механізмі кожен вузол локально екстраполює очікуваний рівень енергії на основі старих (повідомлених) рівнів енергії та рівня споживання енергії для цього вузла на основі останніх двох повідомлених значень. Недоліком алгоритму прогнозування є необхідність чекати двох різних сприйманих показників вартості, тому споживання може бути розраховане і використане

для регулювання сприйнятих значень. Для прогнозування потрібно принаймні два попередніх значення. Якщо вибрано новий MPR, то неможливо передбачити залишкову енергію, оскільки попередні дані недоступні. При великих навантаженнях трафіку коригування трапляються менш рідко. Повідомлення про протокол управління втрачаються/затримуються, і в результаті вузли не будуть "чути" інші вузли. Після того, як вузол вважається недосяжним, фаза запуску знову викликається, коли для розрахунку норми споживання необхідні принаймні два послідовні повідомлення.

Для того, щоб подолати недоліки техніки прогнозування, використовується метод інтелектуального прогнозування, в якому коригування відбуваються майже весь час. Кількість настроювання часу залежить від часу інтервалу пакетів. У алгоритмі Smart Prediction для кожної пари вузлів (p, q), якщо швидкість споживання q ще не відома, p налаштовує сприйняте значення залишкового рівня енергії q на основі середнього значення всіх відомих показників споживання для інших вузлів. Якщо p не знає єдиної норми споживання для інших вузлів, вона змінює сприйнятий рівень енергії q, виходячи з його споживання (p). Використання всіх відомих значень вузлів знижує домінування викидів і забезпечує близькість до реальної норми споживання, припускаючи, що вузли є дещо однорідними за енергетичними характеристиками своїх бездротових карток. Алгоритми прогнозування покращують загальний рівень неточностей при різних трафіку.

Покращення при підвищених показниках трафіку не настільки високе, як і при низьких показниках трафіку. Для того, щоб коректування відбулося, вузол повинен був отримувати дві різні подані значення. Але при підвищених обсягах трафіку, через втрату повідомлення та затримки, зменшується відсоток часу, коли коригування відбувається. Оскільки алгоритм інтелектуального прогнозування вирішує проблему неможливості постійно налаштовувати сприйманий рівень енергетичного рівня, воно досягає

набагато кращої продуктивності з точки зору загальної неточності, особливо при підвищенні трафіку. Обидва алгоритми прогнозування та інтелектуального прогнозування перевершують протокол OLSR за замовчуванням.

У MANET інформація про залишковий рівень енергії, відіграє важливу роль у виборі маршруту. Якщо ця інформація не збирається вузлами, то буде страждати робота мережі. Оцінено ефект часу, на якому зібрана інформація про стан в ідеальному та реалістичному підході. Можна зробити висновок, що навіть якщо ідеальний підхід кращий, ніж реалістичний то збільшення частоти пакетів дуже мало підвищує продуктивність мережі. Крім того, це призводить до збільшення накладних витрат на рух (трафік). Як рішення, використовується механізм прогнозування та механізм інтелектуального прогнозування. Він працює краще, ніж протокол EOLSR, і зменшує завантаження трафіку [11].

2.3 MP-OLSR

Основними завданнями протоколів багатопроменевої маршрутизації є забезпечення надійного зв'язку та забезпечення балансування навантаження, а також підвищення якості обслуговування (QoS) спеціальних і мобільних мереж. Інші цілі протоколів багатопроменевої маршрутизації полягають у підвищенні затримки, зменшенні накладних витрат і максимізації терміну служби мережі.

Кілька шляхів можуть бути використані як резервний маршрут або використовуватися одночасно для паралельної передачі даних (наприклад, кругової). Кілька отриманих шляхів можуть бути згруповані в три категорії:

1. Непересічна: ця група може бути класифікована на вузлово-непересічну і зв`язково-непересічну. У типі багатопроменевого вузла, що не перетинає вузли, не існує спільних вузлів між обчисленими шляхами, які

пов'язують джерело і призначення. Типи багатопроменевих з'єднань, що не перетинаються, можуть розділяти деякі вузли, але всі посилання різні.

2. Поєднана: багатопроменевий тип може спільно використовувати один або більше маршрутів.

3. Гібридні шляхи: поєднання попередніх двох видів [6].

Для покращення маршрутизації протоколу OLSR і існує багатопроменевий протокол MP-OLSR на основі OLSRv2.

На відміну від OLSRv2, MP-OLSR є своєрідним гібридним протоколом багатопроменевої маршрутизації. Подібно до OLSRv2, цей новий протокол змушує кожен вузол періодично надсилати повідомлення Hello та TC і збирати інформацію топології бездротової мережі. Але кожен вузол більше не підтримує таблицю маршрутизації. Замість цього, джерело обчислює весь шлях, коли він повинен відправити пакети, а потім поміщає шляхи в пакети (різні пакети можуть отримати різні шляхи, але один пакет просто отримує один шлях). Взагалі кажучи, інші проміжні вузли просто повинні передати пакет наступному стрибку відповідно до шляху, що переноситься пакетом.

Цей механізм дозволяє уникнути важкого обчислення декількох шляхів кожного разу, коли один вузол отримує повідомлення TC або Hello.

З усіх типів багатопроменевого зв'язку тип вузла «непересічний» є найбільш незв`язний, оскільки всі вузли/ланки двох маршрутів різні, тобто мережевий ресурс є індивідуальним для відповідних маршрутів. Тим не менш, непересічний підхід не завжди є оптимальним рішенням, особливо для розріджених мереж і багатокритеріальних обчислень.

MP-OLSR можна розглядати як різновид гібридного протоколу багатопроменевої маршрутизації, який поєднує проактивні та реактивні особливості. Він періодично надсилає повідомлення HELLO та TC, щоб визначити топологію мережі, як і OLSR. Однак MP-OLSR не завжди зберігає таблицю маршрутизації. Він обчислює лише декілька маршрутів, коли потрібно розсилати пакети даних.

Основна функціональність MP-OLSR має дві частини: топологічне зондування та обчислення маршруту. Топологічне зондування полягає в тому, щоб зробити вузли в курсі інформації топології мережі. Ця частина отримує вигоду з MPRs, як OLSR. Обчислення маршруту використовує алгоритм Дейкстра для обчислення багатопроменевості на основі інформації, отриманої з топологічного зондування. Маршрут джерела (всі переходи від джерела до пункту призначення) зберігається в заголовку пакетів даних.

Визначення топології та обчислення маршруту дозволяють знайти кілька шляхів від джерела до місця призначення. У специфікації алгоритму шляхи будуть доступними і без циклу. Однак на практиці ситуація буде набагато складнішою через зміну топології та нестабільності бездротового середовища. Таким чином, відновлення маршруту та виявлення циклів також пропонуються як допоміжні функціональні можливості для поліпшення продуктивності протоколу. Відновлення маршруту може ефективно знизити втрати пакетів, а виявлення циклу може бути використано для уникнення потенційних циклів в мережі.

Щоб отримати інформацію топології мережі, вузли використовують топологічне зондування, яке включає в себе зондування зв'язку, виявлення сусідів і виявлення топології, як і OLSR. Відчуття зв'язків заповнює локальну інформаційну базу (набір посилань). Це стосується лише адрес інтерфейсу OLSR та можливості обміну пакетами між такими інтерфейсами OLSR. Виявлення сусідів заповнює базову інформацію про сусідство і стосується основних адрес вузлів. Як зондування, так і виявлення сусідів базуються на періодичному обміні повідомленнями HELLO. Відкриття топології генерує інформаційну базу, яка стосується вузлів, які мають більше двох відходів (топологічний набір). Вона базується на затопленні повідомлень TC (оптимізовано шляхом вибору набору MPR).

За допомогою топологічного зондування кожен вузол мережі може отримати достатню інформацію про топологію, щоб забезпечити маршрутизацію. Протокол стану каналу намагається зберегти інформацію

про зв'язок всієї мережі, як згадано вище. За замовчуванням якість шляху вимірюється кількістю стрибків. Він також може бути виміряний іншими показниками, такими як BER (Bit Error Rate) або довжиною черги.

У OLSR маршрути визначаються вузлами кожного разу, коли вони отримують нові повідомлення керування топологією (TC або HELLO). Маршрути до всіх можливих пунктів призначення зберігаються в таблицях маршрутизації. Для MP-OLSR використовується схема на вимогу, щоб уникнути важкого обчислення декількох маршрутів для кожного можливого призначення.

Використовуючи схему топологічного зондування, ми можемо отримати топологічну інформацію мережі з обміну повідомленнями HELLO і TC. Вся ця інформація зберігається в інформаційній базі топології локального вузла: набір зв'язків, набір сусідів або набір топологій. В ідеалі, топологічна інформаційна база може узгоджуватися з реальною топологією мережі. Однак насправді це важко досягти, головним чином через мобільність спеціальної мережі.

По-перше, для повідомлень HELLO та TC існують певні інтервали під час кожної генерації повідомлення (2c для HELLO і 5c для TC за замовчуванням). Протягом цього періоду топологія може змінюватися через рух вузлів. По-друге, коли повідомлення керування (особливо повідомлення TC) передаються в мережі, може статися затримка або зіткнення. Це призведе до того, що контрольне повідомлення застаріло або навіть втрачено.

Обидві ці дві причини, наведені вище, призведуть до невідповідності між топологією реальної мережі та інформаційною базою топології вузла. Це означає, що коли вузол обчислює кілька шляхів на основі інформаційної бази, він може використовувати посилання, які більше не існують, і викликати збій у маршруті.

Для MP-OLSR, ми пропонуємо Route Recovery, щоб подолати недолік вихідної маршрутизації. Принцип дуже простий: перед тим, як проміжний вузол намагається передати пакет до наступного хопу відповідно до

вихідного маршруту, вузол спочатку перевіряє, чи є наступний стрибок у вихідному маршруті одним з його сусідів (шляхом перевірки набору сусідів) . Якщо так, то пакет пересилається нормально. Якщо ні, то можливо, що "наступний скачок" більше не доступний. Потім вузол буде перераховувати маршрут і пересилати пакет за допомогою нового маршруту [6].

Іншою проблемою, викликаною невідповідністю між топологією реальної мережі та локальною інформаційною базою топології вузла, є цикл. У MP-OLSR автори пропонують простий метод, заснований на маршрутизації джерела, для ефективного виявлення циклу без додаткових витрат на пам'ять: після перерахування нового шляху у відновлення маршруту вузол перевіряє, чи є новий контур циклом. Якщо ні, переадресовуйте пакет; в іншому випадку виберіть інший шлях від нового алгоритму Дейкстра. Якщо немає відповідного шляху, відкиньте пакет. Цей метод може ефективно виявити цикл, не витрачаючи додаткового простору пам'яті. Ефективність протоколу покращується, особливо з точки зору наскрізної затримки.

Подібно до OLSRv2, MP-OLSR використовує підрахунок хопу як метрику посилання. У порівнянні з OLSRv2, MP-OLSR отримує невеликий приріст коефіцієнта доставки і значне зменшення затримок з кінця до кінця. Коли мобільність вузлів у мережі збільшується, різниця між 2 протоколами маршрутизації стає все більшою і більшою. Механізм множинного тракту підвищує надійність протоколів маршрутизації.

MP-OLSR і OLSRv2 можуть співпрацювати в одній бездротовій мережі. Це робить розгортання цього нового протоколу набагато простішим, оскільки може використовувати мережу OLSR. Але загальна продуктивність комбінованої протокольної мережі гірша, ніж MP-OLSR. Однією з причин цього є те, що вузли OLSR не мають відновлення маршруту та виявлення циклу. Стратегії маршрутизації відрізняються через точні сценарії. Якщо щільність вузлів OLSR є високою, то для вузлів джерела MP-OLSR краще відправляти пакети до наступного скачка без додавання всього шляху. В

іншому випадку, коли вузли OLSR служать джерелами, а щільність вузлів MP-OLSR велика, нормально для джерела передавати пакети до наступного стрибка і отримати вигоду від відновлення маршруту і виявлення циклу MP-OLSR вузлів.

У порівнянні з іншими реактивними протоколами багатопроменевої маршрутизації, MP-OLSR забезпечує більш коротку затримку передачі завдяки збору інформації топології заздалегідь (Рис. 2.7). Крім того, він може виявити кілька шляхів більш ефективно, без особливих додаткових витрат [12].

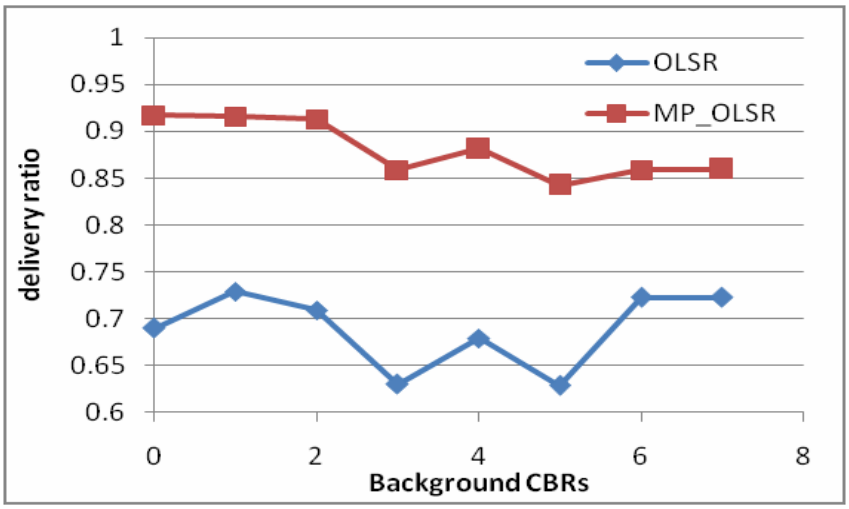

Рисунок 2.7 Коефіцієнт подачі і відповідне стандартне відхилення в OLSR і MP-OLSR

З Рис. 2.7 видно, що MP-OLSR перевершує показник OLSR у співвідношенні доставки при розгляді ефекту фонового трафіку. Перший зберігає коефіцієнт вище 85%, незалежно від того, наскільки важким є фоновий трафік, а другий - на 70%. Кілька шляхів, відновлення маршруту та виявлення циклу допомагають покращити його. При збільшенні фонової CBR зменшується коефіцієнт доставки MP-OLSR. Це може бути результатом більш тривалого часу черги і розчарування деяких шляхів. З точки зору стандартного відхилення коефіцієнта доставки, MP-OLSR показує набагато більш стабільну роботу. Для MP-OLSR середнє стандартне відхилення

становить 0,1, а для OLSR - 0,15. Це можна пояснити зменшенням нестабільності, що виконується кількома шляхами.

MP-OLSR також набагато краще, ніж OLSR, в кінцевій затримці. Його багато з-за багаторазового шляху, що скорочує час чергування в проміжних вузлах. Відновлення маршрутів і виявлення циклу також мають значення. Зі збільшенням фонових CBR, затримки обох протоколів маршрутизації стають більшими. У порівнянні з MP-OLSR, OLSR має більші зміни, особливо в 4-фоновій точці CBR. Цей різкий приріст пояснюється в основному унікальністю сценарію. Але немає сумніву, що MP-OLSR може краще мати справу з незадовільною топологією мережі. Стандартне відхилення також підтримує це: з Рис 2.8 видно, що MP-OLSR має меншу величину для стандартного відхилення, особливо якщо існує більше 5 фонових CBR [12].

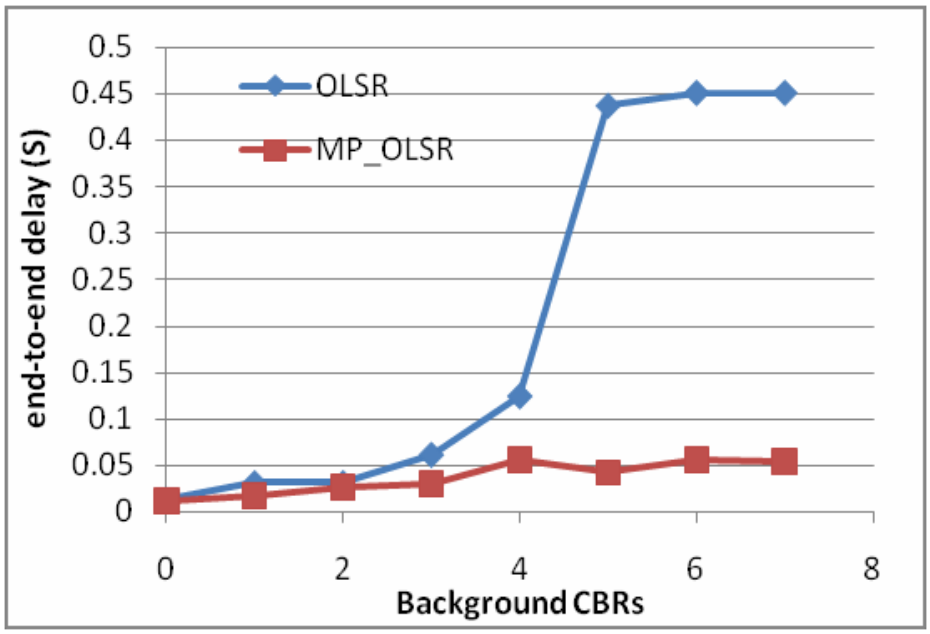

Рисунок 2.8 Наскрізна затримка і відповідне стандартне відхилення в OLSR і MP-OLSR

2.4 SU-OLSR

Suspect Optimized Link-State Routing (SU-OLSR) - новий протокол на основі OLSR, який застосовується для вирішення атак на підміну каналів і

зменшення впливу шкідливих вузлів, які змушують своїх сусідів вибирати їх як MPR. SU-OLSR використовує нову методику вибору MPR на основі довіри до сусідніх вузлів. Методи вибору MPR спрямовані на поліпшення затоплення контрольних повідомлень або для забезпечення високої якості обслуговування [1].

1. Класичні схеми вибору MPR.

Евристика, запропонована в цій групі є діаграмами, заснованими на оригінальному варіанті вибору. Мета полягає в тому, щоб поліпшити деякі показники, пов'язані з впливом на MPR в мережі. Наприклад, оптимізація вибору MPR, зменшення кількості зіткнень через велику кількість обраних MPR або зменшення енергії, що використовується вузлами.

Існують підходи або для зменшення кількості MPR, і для обмеження зіткнення в мережі або для зменшення складності алгоритму вибору MPR.

- За ступенем «Потребуючий зафіксувати покриття»

Мета цього підходу полягає в тому, щоб вибрати максимальну кількість MPR, для зниження обчислювальної складності MPR і збільшити швидкість алгоритму вибору. Цей алгоритм використовує той самий підхід, що й оригінальна евристика для покриття ізольованих вузлів. На другому етапі, поки ще є непокриті вузли в $N_2(S)$, алгоритм у випадковому порядку приймає один з цих вузлів (назвемо цей вузол y). Потім він шукає вузол x в $N_1(S)$ як $y \in N_1(x)$ і x примикає до мінімуму непокритих вузлів з $N_2(S)$.

- Вибір з мінімальним перекриттям

Оригінальна евристика не враховує проблеми зіткнення MPR. Метою цього підходу є розподіл вибраних MPR навколо вузла-джерела для обмеження числа колізій в мережі. Перша фаза вибору MPR, що охоплює ізольовані вузли, є такою ж, як і вихідна схема. Коли є ще 2-хоп вузли вузла S, ми вибираємо як MPR вузол x в $N_1(S)$ який охоплює мінімум вузлів у $N_2(S)$ які ще не охоплені MPR.

- Вибір з вторинним пріоритетом

Метою цього алгоритму вибору є зниження ступеня перекриття MPR без зменшення їх кількості і тим самим обмеження кількості колізій в мережі. Перша фаза вибору MPR S, що охоплює ізольовані вузли, є такою ж, як і вихідна схема. На другому етапі, коли є ще кілька вузлів в $N_1(S)$ що охоплюють однакову кількість вузлів у $N_2(S)$, алгоритм обраний як MPR вузла в $N_1(S)$ який має мінімум сусідів в $N_2(S)$.

- Випадковий вибір

Варіант пропонує випадково вибирати MPR серед вузлів, які охоплюють однакову кількість вузлів $N_2(S)$.

Інший підхід був запропонований компанією Lipman. Вона полягає в прагненні мінімізувати маршрутизацію повідомлень і врахувати певні характеристики вузлів (енергію, корисність порівняно з сусідами) при розрахунку MPR [13].

2. Схеми на основі пов'язаних домінуючих множин

Цей підхід полягає в зменшенні кількості вузлів, що беруть участь у маршрутизації повідомлень, шляхом побудови відповідних домінуючих наборів MPR. Дві евристики використовують цей підхід [14].

Перша евристика була запропонована для обчислення пов'язаних домінуючих множин MPR. Домінуючий набір обчислюють з MPR, отриманих з використанням вихідного алгоритму вибору MPR. Іншими словами, спочатку необхідно обчислити набір MPR, використовуючи класичний алгоритм перед обчисленням пов'язаних домінуючих множин MPR [15].

Покращено попередню евристику, щоб генерувати невеликі домінуючі зв'язані множини MPR. Це вдосконалення ґрунтується на оригінальному алгоритмі вибору MPR, але використовує інформацію 3-хопу вузла для обчислення MPR, які охоплюють більшість 2-хоп вузлів [16].

3. Схеми, засновані на якості обслуговування

Запропонована евристика з урахуванням якості обслуговування (QoS) або іншими словами, для вибору MPR, які гарантують певний QoS. Такий підхід буде корисним у мережах, де якість обслуговування є надзвичайно важливою (VoIP, відео, додатки, що вимагають невеликих затримок і т.д.).

Є два підходи для вирішення питання про обмеження початкової евристики в термінах QoS. Метою цих підходів є вибір MPR на основі метрик QoS (затримка, пропускна здатність). Вузли, які пропонують велику пропускну здатність або мінімум затримки, будуть сприятливі для вибору MPR під час механізму вибору MPR [17].

Є запропонований підхід, щоб гарантувати, що всі вузли з двома хопами вихідного вузла мають оптимальний шлях з точки зору смуги пропускання до вихідного вузла. Для будь-якого 2-хоп-вузла S-вузла, вузол в $N_1(S)$, що пропонує найширшу смугу пропускання по відношенню до S обраний як MPR. Таким чином ми охоплюємо всі вузли $N_2(S)$ за допомогою MPR, які пропонують широку смугу пропускання [18].

2.5 Висновки з розділу 2

В даному розділі аналізується робота деяких модифікацій протоколу OLSR. Були розглянуті причини введення цих протоколів. В ході цього розділу показано, як та чи інша модифікація протоколу OLSR усуває певні недоліки основного протоколу.

Визначено, що саме MPR відіграють важливу роль у оптимізації доставки повідомлень у протоколі OLSR. Однак типи вузлів в цьому протоколі є невралгічними точками мережі і недовіра до цих вузлів буде мати дуже важливий вплив на загальне функціонування мережі. Дійсно, шкідливий вузол, який був обраний як MPR своїми сусідами, має повний контроль над усіма повідомленнями, які проходять через нього. Таким чином, він може змінити або взагалі відхилити їх. Зловмисний вузол може

навіть навмисно змусити своїх сусідів вибирати його як MPR, наприклад, за допомогою методів підміни каналів. Саме SU-OLSR допомагає вибирати правильні MPR для того, щоб мінімізувати кількість підозрілих вузлів в мережі. Тому наступний розділ присвячується протоколу SU-OLSR.

3 ПРОТОКОЛ SU-OLSR

MPR відіграють важливу роль у оптимізації доставки повідомлень у протоколі OLSR. Однак типи вузлів в цьому протоколі є невралгічними точками мережі і недовіра до цих вузлів буде мати дуже важливий вплив на загальне функціонування мережі. Дійсно, шкідливий вузол, який був обраний як MPR своїми сусідами, має повний контроль над усіма повідомленнями, які проходять через нього. Таким чином, він може змінити або взагалі відхилити їх. Зловмисний вузол може навіть навмисно змусити своїх сусідів вибирати його як MPR, наприклад, за допомогою методів підміни каналів.

Вузол не повинен довіряти сусідньому вузлу *x*, який має шкідливі характеристики, що може вплинути на вибір MPR.

Нехай S заданий вузол мережі. Вказаний вузол $x \in N_1(S)$ відповідає критерію I або критерію II, якщо:

- Критерій I: вузол *x* охоплює один або кілька ізольованих вузлів в $N_2(S)$.
- Критерій II: вузол *x* охоплює частку вузлів у $N_2(S)$, до яких немає доступу у інших.

Вузол вважається підозрілим, якщо він містить підозрілу поведінку відповідно до одного з цих критеріїв. Для кожного вузла *S* ми також визначаємо набір вузлів *x*, які виявляють підозрілу поведінку по відношенню до нього наступним чином:

$$Підозрілий(S) = \{X \in N_1(S) \mid X \text{ є підозрілим}\} \quad (3.1)$$

3.1 Новий алгоритм вибору MPR

Протокол SU-OLSR використовує новий алгоритм вибору MPR. Метою цього алгоритму є визначення сукупності підозрілих вузлів.

Для будь-якого вузла S, заданого в мережі, ми спочатку знаходимо всі його сусіди при 1-хоп та 2-хоп стрибках (N_1 (*S*) та N_2 (*S*)). Потім шукаємо вузли *x* в $N_1(S)$, які демонструють підозрілу поведінку відповідно до критеріїв I або II. Якщо такі є, ми додаємо знайдені вузли до підозрюваних *Підозрілий(S)*.

Наступним кроком алгоритму є перегляд сусідів на 1-хоп стрибку S (без підозрілих):

$$N^*_1(S) = \{y \in N_1(S) \setminus Підозрілий(S)\}, \quad (3.2)$$

і всіх сусідів на 2-хоп стрибку на основі набору $N_1^*(S)$ і визначаємо:

$$N^*_2(S) = \{z | z \neq S \wedge z \notin N^*_1(S) \wedge (\exists y \in N^*_1(S))\,[z \in N_1(y)]\}. \quad (3.3)$$

З наборів $N^*_1(S)$ та $N^*_2(S)$ до набору MPR додаємо кожен вузол з $N^*_1(S)$, який охоплює ізольований вузол в $N^*_2(S)$ і виключаємо вузли в $N^*_2(S)$, а також вузли, покриті одним з MPR, обраного на цьому етапі. Поки всі вузли в $N^*_2(S)$ не всі покриті, до набору MPR додаємо вузол $N^*_1(S)$, який охоплює максимум вузлів у $N^*_2(S)$. Таким чином, набір надійних MRP вузла S, а також всі підозрілі вузли розраховуються відповідно до алгоритму, що відноситься до SU-OLSR. Ми також визначаємо сукупність сусідів, які оголосили надійним *z* вузол:

$$Sel_{MPR}(z) = \{y \in N_1(z)\; z \in MPR(y)\}. \quad (3.4)$$

Точно так само всі сусіди *z*-вузла, які оголосили його небезпечними, визначаються:

$$Sel_{Suspects}(z) = \{y \in N_1(z)\; z \in Suspects(y)\}. \quad (3.5)$$

Données : Tout nœud s avec ses voisins $N_1(s)$ et $N_2(s)$.
Résultat : Les ensembles $MPR(s)$ et $Suspects(s)$.

début
  $Suspects(s) \leftarrow \emptyset$;
  pour *tout nœud* x *dans* $N_1(s)$ **faire**
    si x *démontre le critère choisi* **alors**
      Ajouter x à $Suspects(s)$;
    fin
  fin
  $N_1^*(s) \leftarrow N_1(s) \backslash Suspects(s)$;
  $N_2^*(s) \leftarrow$ voisins à $2-$sauts basés sur $N_1^*(s)$;
  $MPR(s) \leftarrow \emptyset$;
  pour *tout nœud* y *dans* $N_2^*(s)$ *isolé* **faire**
    Soit $x \in N_1^*(s)$ le seul voisin de ce nœud y;
    Ajouter x à $MPR(s)$;
    Éliminer tous les nœuds dans $N_2^*(s)$ couverts par x;
  fin
  tant que $N_2^*(s) \neq \emptyset$ **faire**
    Trouver $x \in N_1^*(s)$ tq.
    - x couvre le maximum des nœuds dans $N_2^*(s)$;
    - x a le maximum des voisins ;

    Ajouter x à $MPR(s)$;
    Éliminer tous les nœuds dans $N_2^*(s)$ couverts par x;
  fin
fin

Рисунок 3.1 Алгоритм вибору MPR по SU-OLSR

На рисунку 3.2 наведено порівняння між алгоритмом вибору MPR для SU-OLSR та класичним визначенням. Вузли 1, 3 і 7 визнані небезпечними за протоколом SU-OLSR.

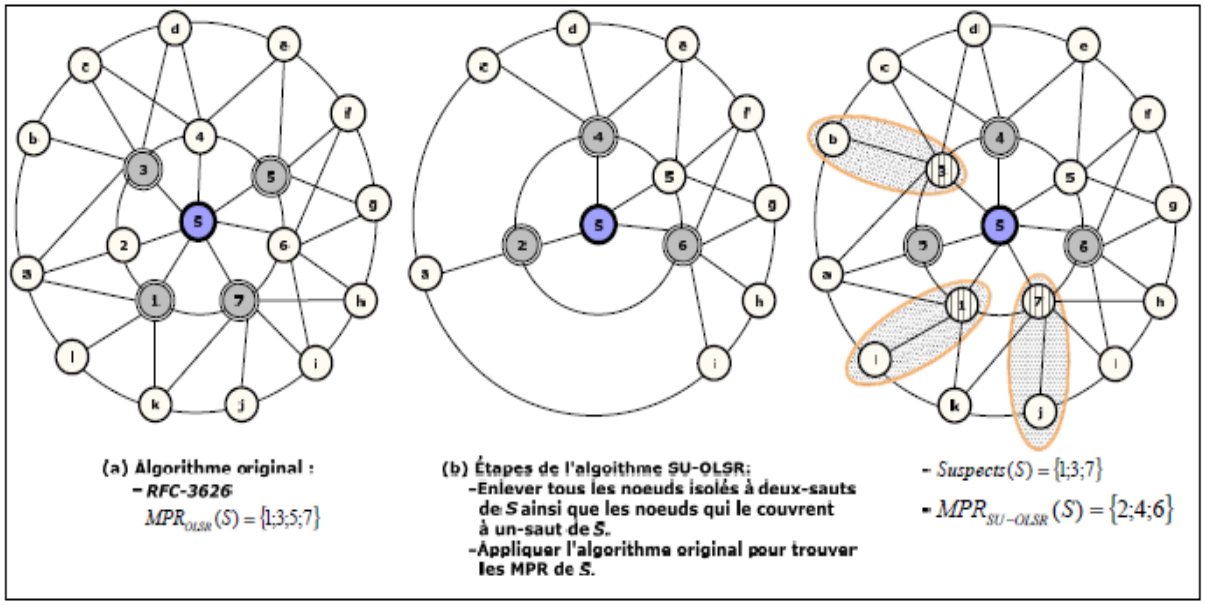

Рисунок 3.2 Застосування алгоритму вибору SU-OLSR MPR

Алгоритм вибору MPR SU-OLSR заснований на виборі надійних вузлів. Деякі легітимні вузли можуть мати характеристики Критерію I (наприклад, законний вузол, який охоплює легітимний ізольований вузол (неіснуючий вузол в мережі або віддалений)). Вони можуть бути визнані небезпечними. З іншого боку, деякі вузли в $N_2(S)$ по-іншому не могли бути приєднаними.

На рисунку 3.2 вузол *k* являє собою побічний варіант вибору SU-OLSR, оскільки єдині вузли в $N_1(S)$, які охоплюють його, оголошуються підозрілим вузлом S. Все це вплине на шляхи між легітимними вузлами в мережі. Але з мережею, яка має певну щільність, графік топології буде з'єднаний.

3.2 Повідомлення керування та алгоритм потоку в SU-OLSR

Коли всі надійні та підозрілі MPR в мережі були розраховані, необхідно визначити механізм для поширення топологічної інформації в мережі.

Протокол SU-OLSR використовує ті самі механізми потоку, що й класичний протокол OLSR. Єдині зміни стосуються форматів та вмісту повідомлень HELLO та TC. Повідомлення керування необхідно змінити, щоб розглянути інформацію про механізм довіри. Дійсно, в SU-OLSR, необхідно, щоб кожен вузол *S* в мережі надавав у своїх повідомленнях HELLO інформацію про довіру до MPR, а також інформацію про підозрілі вузли надану сусідами. Точно так само необхідно, щоб кожен вузол, що випромінює повідомлення, у TC повідомляв про вузли, які вибрали його як надійний MPR, а також вузли, які оголосили його підозрілими. Це призводить до розподілу наборів *SelMPR(S)* і *SelSuspects (S)* у повідомленнях TC вузла S. Ця зміна форми контрольних повідомлень не впливає на навантаження в мережі в порівнянні з класичний протокол OLSR.

Оскільки топологічна інформація обмінюється між вузлами відповідно до нових специфікацій контрольних повідомлень SU-OLSR, кожен вузол

повинен обчислити найкоротші шляхи до даного пункту призначення, використовуючи алгоритм Дейкстра. Для кожного вузла існує два варіанти обчислення його шляхів, які визначаються таким чином:

• Варіант I: Використовуйте для розрахунку правильних маршрутів MPR, які декларуються безпечно всіма вузлами мережі.

• Варіант II: Використовуйте для розрахунку своїх маршрутів MPR, які оголошені безпечними певними вузлами мережі.

Іншими словами, можна класифікувати MPR, що використовуються вузлами в SU-OLSR, для обчислення шляхів і маршрутизації повідомлень у дві категорії: повні довірені MPR:

$$MPR_{\text{всі}} = \{x | Sel_{MPR}(x) \neq \emptyset \wedge Sel_{Suspects}(x) \neq \emptyset\}, \quad (3.6)$$

та частково довірені MPR:

$$MPR_{\text{часткові}} = \{x | Sel_{MPR}(x) \neq \emptyset\} \quad (3.7)$$

Розрахунок шляхів, беручи до уваги варіант I або варіант II, впливатиме на довжину маршруту та характер графіка MPR.

3.3 Аналіз моделі атаки

Впровадження протоколу SU-OLSR вимагає трьох гіпотез, щоб гарантувати ефективність нашого рішення:

1. Кожен законний вузол міг підписати свої контрольні повідомлення за допомогою свого попередньо визначеного криптографічного ключа. [19]

2. Не існує взаємодії між шкідливими вузлами.

У випадку, коли два зловмисних вузла співпрацюють в мережі, вони можуть заявити, що вони охоплюють один і той же неіснуючий вузол в мережі, щоб переконатися, що один з них обраний як MPR.

3. Всі вузли мережі оснащені єдиним бездротовим мережевим інтерфейсом.

У випадку, коли зловмисний вузол має два бездротові мережеві інтерфейси, він може оголосити кожним своїм інтерфейсом, що він охоплює неіснуючий вузол, а два інтерфейси, що використовуються цим вузлом, розглядаються іншими вузлами як два різних вузла. Отже, без сумніву, він буде обраний як MPR одним із сусідів.

Завдяки протоколу SU-OLSR, шкідливий вузол, який заявляє, що він охоплює ізольований або віддалений вузол, невідомий іншими сусідами, ніколи не буде обраний як MPR. Єдині можливості, які йому залишаються, - це брехати про його справжній статус у мережі. Для того, щоб оцінити SU-OLSR при наявності шкідливого вузла, передбачається, що вузли можуть брехати щодо свого статусу в мережі.

У першому випадку маються на увазі, що зловмисний вузол *m* заявляє, що він був обраний одним зі своїх сусідів *x*, як небезпечний вузол. У цьому випадку шкідливий вузол не отримує вигоди від будь-якої позиції в мережі, оскільки він оголошується іншими вузлами як небезпечними для передачі їх повідомлень.

У другому випадку ми припускаємо, що зловмисний вузол *m* заявляє, що він був обраний як довірений MPR вузлом *x*. Проте, в разі, коли x є одним з *m* сусідів або знаходиться в тій же зв'язковий частини графа мережі, то вузол *x* повинен отримувати повідомлення TC, що генеруються зловмисним вузлом, і в якому він стверджує, що *x* вибрав його як довірений MPR. Після отримання цих повідомлень TC вузол *x* може ініціювати механізм контрзаходів, щоб денонсувати зловмисний вузол до інших вузлів.

З іншого боку, неможливо виявити цю атаку, якщо вузол *x* і шкідливий вузол не знаходяться в тій самій зв'язаній частині мережі. Дійсно, оскільки *x* не знаходиться в зв'язаному графі *m*, він ніколи не отримає TC-повідомлень управління *m*. Таким чином, неможливо буде встановити механізм контрзаходів для денонсування зловмисного вузла. Це являє собою обмеження на наше рішення в тому випадку, якщо мережевий граф не пов'язаний. Щоб вирішити цю проблему потрібно вважати, що наша мережа

достатньо щільна, щоб мережевий граф був пов'язаний. У цьому випадку ефективність попередження атаки гарантується механізмом контрзаходів. Загаломих вузлів, ми завжди можемо знайти шлях, який з'єднує два легітимн, якщо мережний граф є *k+1* підключений і існує наявність *k* зловмисн і вузли і не проходить через один з шкідливих вузлів. Ця пропозиція випливає з теореми: *якщо щільність вузлів у мережі є досить великою, щоб мати граф (k + 1) - підключений, то, якщо ми видалимо k вузли мережі, граф залишається завжди з'єднаним* [20].

3.4 Експериментальна оцінка SU-OLSR

У SU-OLSR будь-який вузол з підозрілою поведінкою за нашими двома критеріями не може бути обраний як MPR за алгоритмом SU-OLSR. Однак деякі легітимні вузли не можуть бути обрані як MPR за протоколом. Це матиме вплив на підключення до мережі.

Ми будемо аналізувати та порівнювати продуктивність SU-OLSR і OLSR у випадку мережі з фіксованими вузлами завдяки програмі, розробленій на C і, нарешті, у випадку динамічної мережі завдяки Network Simulator 2 (NS-2).

1. Параметри оцінки

- Затримка від кінця до кінця:

Це дається затримкою передачі плюс затримкою поширення. Іншими словами, це час, який пакет проходить між джерелом і кінцевим пунктом. Протокол має кращу продуктивність, якщо він гарантує невелику затримку з кінця до кінця.

- Відсоток доставлених пакетів:

Packet Delivery Ratio (PDR) - це показник, який обчислює загальну кількість пакетів, що доставляються до пункту призначення, на основі кількості відправлених пакетів.

- Кількість стрибків:

Кількість переходів, що приймає пакет, щоб перейти від вихідного вузла до місця призначення. Цей параметр використовується для визначення продуктивності протоколів щодо знайдених оптимальних шляхів.

- Вплив щільності:

Для кожного моделювання ми генеруємо множину N з 100 вузлів, розподілених випадково в квадраті 1000м х 1000м. Для даного радіуса зв'язку R цей набір точок визначає неорієнтований граф G(R) =(N , E_R), з:

$$E_R = \{(a,b)|a,b \in N \wedge d_2(a,b) \leq R\}, \quad (3.8)$$

де d_2 - Евклідова відстань між двома точками в площині.

Властивості цього типу графа були вивчені в теорії випадкових геометричних графів. Найбільш цікавим результатом цієї теорії є те, що граф, що складається з n вузлів, пов'язаний з максимальною ймовірністю, якщо радіус зв'язку його вузлів принаймні дорівнює [21]:

$$\sqrt{\frac{\ln n + O(1)}{\pi n}} \quad (3.9)$$

Отже, граф пов'язаний з ймовірністю $1 - \frac{1}{s}$, якщо радіус зв'язку вузлів більше[22]:

$$\sqrt{\frac{\ln n + \ln s}{\pi n}} \quad (3.10)$$

Отже, у нашому випадку граф G(r) пов'язаний з ймовірністю більше 99%, якщо радіус зв'язку вузлів r більше 171 м. Отже, під час нашого моделювання ми помітили, що якщо радіус зв'язку вузлів більше або дорівнює 190 м, графік зазвичай з'єднується або має дуже мало ізольованих вузлів. Саме з цієї причини у всіх наших моделюваннях ми будемо використовувати промені, що перевищують або дорівнюють 190 м для забезпечення гарного зв'язку між вузлами.

3.5 Модель без мобільності

Метою в цій частині є оцінка нашого протоколу в простому середовищі, де всі вузли фіксовані. Оцінка включає обчислення кількості MPR для двох протоколів, кількості повідомлень TC, що генеруються вузлами, і, нарешті, обчислення найкоротшого шляху між вузлами в мережі.

Для цього модулюється два протоколи SU-OLSR і OLSR завдяки програмі, розробленій на мові C. Метою є створення платформи для моделювання для двох протоколів (алгоритми вибору та алгоритм найкоротшого шлях).

Наша програма імітує стандартні протоколи SU-OLSR і OLSR на площі 1 км^2, де всі вузли фіксовані. Виконання двох протоколів вивчається в різних відділах зв'язку. Результати кожного експерименту є результатом в середньому 50 незалежних симуляцій. Це забезпечує більш високий довірчий інтервал. У кожному моделюванні позиції вузлів топології генеруються випадковим і незалежним чином.

У Табл. 3.1 наведено резюме параметрів статичного моделювання.

Таблиця 3.1 Статичне моделювання

Сценарій	Топологія	Промені зв'язку	Повторення
Статичний	1000*m x* 1000*m*	190, 250, 290, 330, 390 m	50 моделювань на радіус
Кількість симуляцій на протокол			50 ∗ 5 = 250 моделювань

- Кількість MPR

Новий протокол SU-OLSR та його алгоритм вибору впливають на кількість MPR в мережі. Важливо потім порівняти кількість MPR, вибраних двома звичайними протоколами SU-OLSR і OLSR.

Під час моделювання статичного режиму протоколу OLSR ми помітили, що на першій фазі алгоритму вибору вибирається велика кількість MPR. Таблиця 3.2 дає загальну кількість вузлів, які вибрали MPR, що охоплює ізольований вузол (1), загальна кількість MPR, що охоплюють ізольовані вузли (2), середнє число на вузол MPR, що працюють на ізольованих вузлах (3). Ці результати показують, що більш ніж 75% MPR вибираються на першій фазі алгоритму. Однак ця фаза є критичною для нового алгоритму вибору MPR протоколу SU-OLSR. Дійсно, деякі легітимні вузли не можуть бути обрані як MPR, якщо вони охоплюють один або більше ізольованих вузлів (див. пункт 3.1).

Таблиця 3.2 Кількість MPR, що охоплюють ізольовані вузли

Промені зв'язку	(1)	(2)	(3)
190 *m*	96.0	48.8	2.41
290 *m*	97.5	44.1	2.48
390 *m*	90.7	33.3	1.85
490 *m*	56.8	17.6	0.89
590 *m*	14.0	4.7	0.15
690 *m*	0.8	0.3	-

На Рис. 3.1 показано, залежно від радіусу зв'язку, середнє число MPR, вибраних за протоколом SU-OLSR з Критерієм I (Варіант I і Варіант II) і звичайним протоколом OLSR. Ця цифра показує, що у випадку варіанту I кількість MPR, вибраних SU-OLSR, набагато нижче, ніж кількість MPR, вибраних за звичайним протоколом OLSR. Це не дивно, тому що алгоритм SU-OLSR може вибирати тільки MPR, визнані безпечними всіма вузлами.

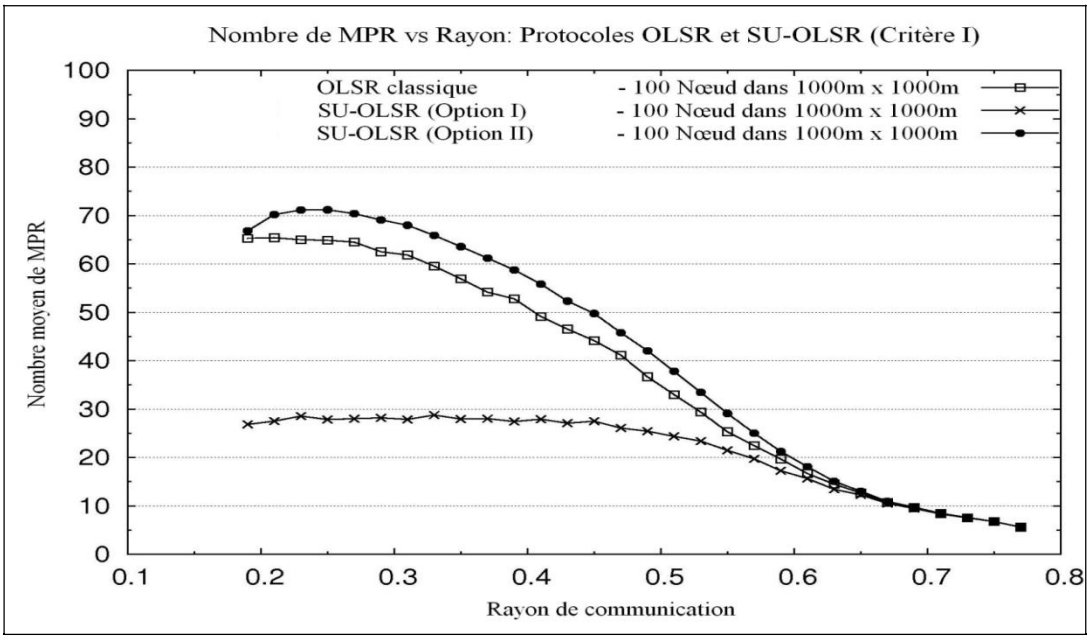

Рисунок 3.1 Порівняння кількості MPR у випадку критерію I

У випадку варіанту II кількість MPR, вибраних SU-OLSR, більше, ніж кількість MPR, вибраних OLSR. У цьому випадку велика кількість MPR не обов'язково означає, що графік, що представляє топологію, більше пов'язаний, ніж той, який отриманий у випадку протоколу OLSR. Можуть бути однорангові вузли, які більше не підключені при використанні SU-OLSR. Дійсно, якщо вузол x був обраний як захищений MPR вузлом a і небезпечним MPR іншим вузлом b, то до графа, який використовується алгоритмом Дейкстра, додається тільки орієнтована дуга $x \rightarrow a$ для розрахунку найкоротшого шляху. У той час як у випадку протоколу OLSR додаються дві орієнтовані дуги $x \rightarrow a$ та $x \rightarrow b$.

У випадку Критерію II параметри щільності та коефіцієнт, який представляє максимальну фракцію, яку може охоплювати вузол, повинні змінюватися. Тепер у топології, де вузли розподілені випадковим чином, вузол у в $N_1(x)$ охоплює в ідеальному випадку співвідношення 20% сусідів з двома стрибками x. У деяких випадках цей відсоток може досягати 40%.

Дійсно, якщо розглядати вузли з радіусом зв'язку R, область області, що містить сусіди з 2-хопами x, задається

$$\text{Поверхня}_{N_2} = \pi(2R)^2 - \pi R^2 = 3\pi R^2 \qquad (3.11)$$

Однак у випадку, коли *y* знаходиться на відстані *R* *x* (див. Рис. 3.2-a), площа області Поверхня_{N_1}, що містить N1(y), максимальна. Потім ми маємо наступне рівняння:

$$\text{Поверхня}_{N_1} \leq \pi R^2 - \left(2R^2\frac{\pi}{3} - \frac{\sqrt{3}}{2}R^2\right) = (\frac{\pi}{3} + \frac{\sqrt{3}}{2})R^2. \qquad (3.12)$$

Отже, в ідеальному випадку (Рис. 3.2-a) співвідношення цих двох поверхонь задається:

$$\text{Співвідношення}_{\text{ідеал}} \leq \frac{(\frac{\pi}{3}+\frac{\sqrt{3}}{2})R^2}{3\pi R^2} = \frac{2\pi+3\sqrt{3}}{18\pi} \leq 0.203 \qquad (3.13)$$

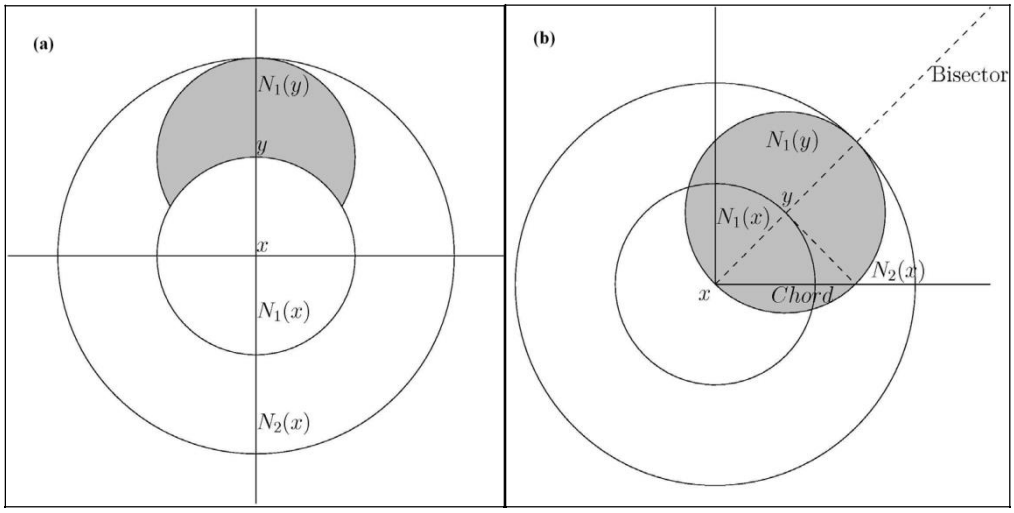

Рисунок 3.2 Зональна зона охоплення

Якщо вузол *x* знаходиться на межі модельованої області, то співвідношення визначається як:

$$\text{Співвідношення}_{\text{межа}} \leq \frac{2(\frac{\pi}{3}+\frac{\sqrt{3}}{2})R^2}{3\pi R^2} = \frac{2\pi+3\sqrt{3}}{9\pi} \leq 0.406 \quad \text{(див. Рис. 3.2-b)}$$

Потім коефіцієнт встановлюється на рівні 25% у нашому моделюванні. Іншими словами, вузол може бути максимально підключений до чверті числа 2-хоп вузлів даного вузла. На рисунку 4.3 видно, що кількість MPR, вибраних SU-OLSR та OLSR, є однаковими, коли радіус зв'язку більше 300 м. Іншими словами, SU-OLSR з Критерієм II (Варіант I і Варіант II) не відкидає жодного

законного вузла. Для радіусів зв'язку менше 300 м слід зазначити, що кількість повністю захищених MPR, вибраних SU-OLSR (Варіант I), менше, ніж кількість MPR, вибраних традиційним протоколом OLSR.

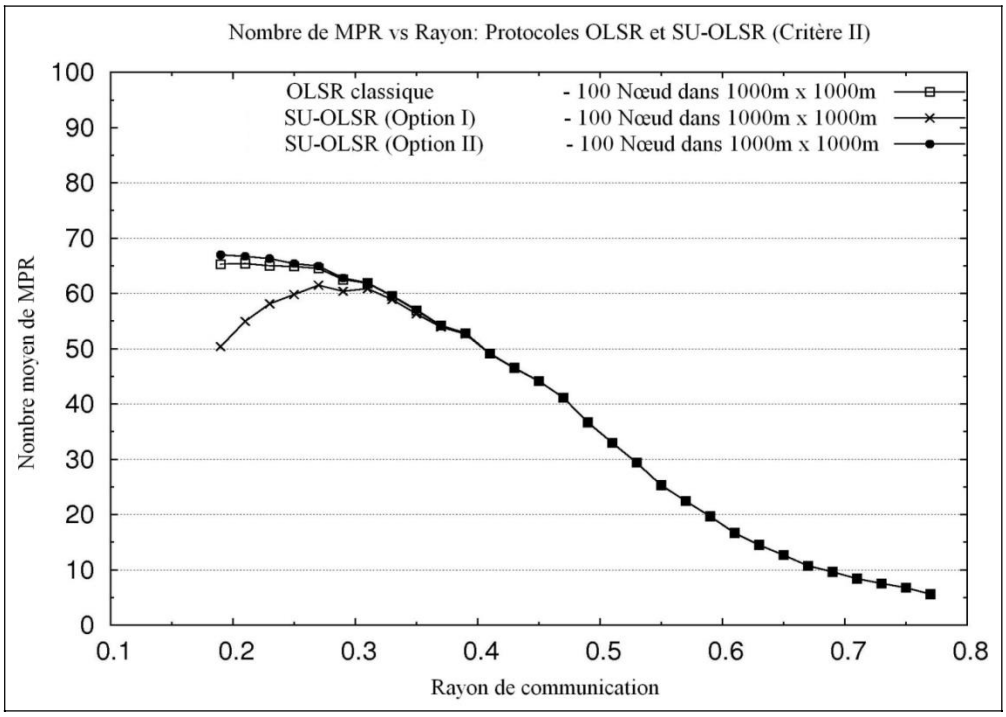

Рисунок 3.3 Кількість MPR у випадку Критерію II з коефіцієнтом 0.25

- Кількість повідомлень TC

Кількість вибраних MPR має прямий вплив на кількість повідомлень TC, що транслюються в мережі. Дійсно, кожен MPR повинен періодично надсилати повідомлення TC, щоб оголосити вузли, які обрали його, як безпечне або небезпечне багатоточкове реле. Цей тип повідомлення транслюється іншими MPR. Для того, щоб обмежити навантаження трафіку в мережі, кожне TC-повідомлення, що генерується MPR, транслюються один раз у часовий інтервал іншими MPR.

Кількість TC повідомлень - це квадрат кількості MPR в мережі. На Рис.3.4 наведено порівняння кількості TC повідомлень, що генеруються у випадку двох протоколів SU-OLSR (Критерій I) і OLSR. Слід зазначити, що у випадку SU-OLSR з використанням Критерію I і I варіанту, кількість TC

повідомлень зменшується приблизно на 33% порівняно з кількістю повідомлень, що генеруються у разі використання протоколу OLSR.

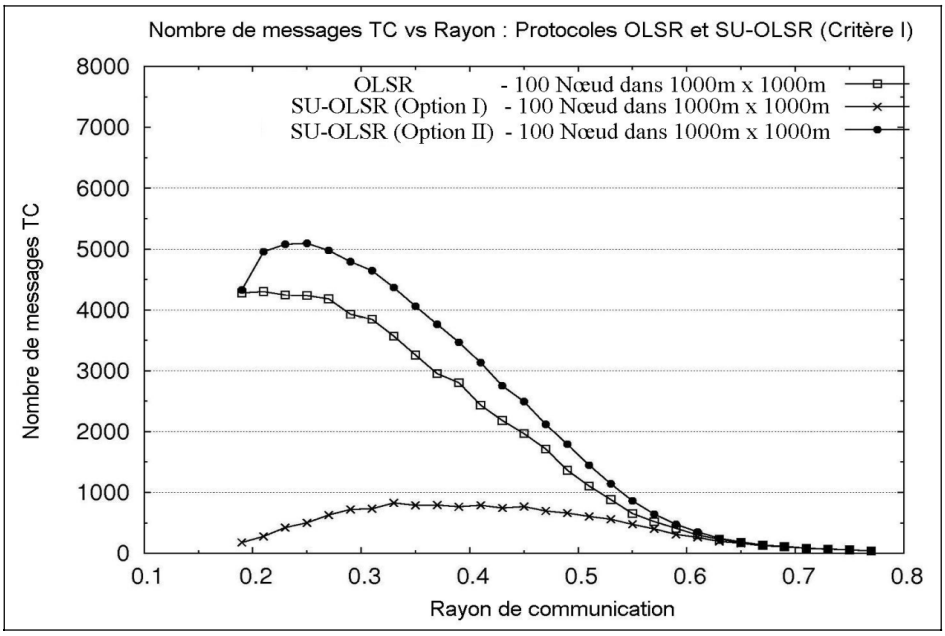

Рисунок 3.4 Порівняння кількості генерованих повідомлень TC

- Найкоротший шлях між вузлами

Продуктивність протоколу залежить, зокрема, від довжини найкоротших шляхів між вузлами в мережі. Цей показник безпосередньо впливає на затримку з кінця до кінця, перевантаженість у мережі та відсоток втрачених пакетів. Тому важливо проаналізувати та порівняти вибір найкоротших шляхів SU-OLSR у порівнянні з традиційним протоколом OLSR.

Після того, як зроблено крок вибору MPR, кожен вузол обчислює ці шляхи до всіх вузлів мережі. Таким чином, кожен вузол будує орієнтований граф, що представляє його бачення всієї топології мережі. Іншими словами, вузол обчислює граф, визначений за допомогою: $G(s) = \langle N(s), E_{N_1}(s) \cup E_{N_2}(s) \cup E_{MPRSel} \rangle$ з:

- N (s) є підмножиною вузлів, відомих s.
- $E_{N_1}(s) = \{(s,x) | x \in N_1(s)\}$

- $E_{N_2}(s) = \{(x,y) | \, x \in N_1(s) \wedge y \in N_1(x)\}$
- $E_{MPRSel} = \{(a,b) | \, b \in Sel_{MPR}(a)\}$

Зауважимо, що набір E_{MPRSel} не залежить від s, а тільки від набору MPR ($MPR_{загальні}$ та $MPR_{часткові}$). Алгоритм Дейкстра потім дозволяє обчислити найкоротший шлях між заданим вузлом s і всіма вузлами призначення в мережі.

Випадок варіанту I:

Починаючи з критерію I (немає ізольованого вузла). Ми розглядаємо тільки MPR, оголошений безпечним всіма вузлами. Таким чином, як було показано раніше (див. Рис. 3.1), протокол SU-OLSR вибирає менше MPR, ніж звичайний протокол OLSR. Це впливає на зв'язність графа і кілька пар вузлів не пов'язані в разі мережі з низькою щільністю з використанням SU-OLSR. У цьому випадку найкоротший шлях між двома вузлами буде дуже великим порівняно з традиційним протоколом OLSR.

У таблиці 4.3 наведено відсоток пар вузлів, що їх найкоротший шлях збільшується на один крок Δ. Останній рядок (Δ=∞) являє собою відсоток пар вузлів, для яких протокол SU-OLSR не знаходив шляху, на відміну від OLSR. Результати цієї таблиці підтверджують незв'язаний характер результуючого графіка SU-OLSR. Дійсно, щоб мати пов'язаний графік, вам потрібен радіус зв'язку не менше 390 м. Для цього радіуса SU-OLSR не знаходить дійсного шляху для 4,8% його вузлів (див. Табл. 3.3). Хоча в тих же умовах OLSR просто потребує радіус зв'язку 190 м.

Таблиця 3.3 Довжина шляхів SU-OLSR (критерій I + Варіант I) проти OLSR

Δ	190 *m*	250 *m*	330 *m*	390 *m*
0	0.3128	0.5357	0.8007	0.9198
1	0.0210	0.0486	0.0560	0.0276
2	0.0053	0.0188	0.0198	0.0069
3	0.0016	0.0073	0.0071	0.0020
4	0.0005	0.0031	0.0026	0.0006
≥ 5	0.0002	0.0025	0.0017	0.0007
∞	0.6586	0.3843	0.1120	0.0480

Ці результати показують, що SU-OLSR з критерієм I і варіантом I є дуже дорогим і, це безсумнівно, вплине на споживання енергії обладнання, а також на їх вартість.

Тепер перейдемо до Критерію II (Відсоткове покриття). Використання SU-OLSR в даному випадку аналогічне протоколу OLSR (див. Рис. 3.3). Це відображено в результатах на різниці в довжині шляху між двома протоколами (див. Табл. 3.4). З радіусом зв'язку 250 м і коефіцієнтом 25%, що SU-OLSR не може знайти шляху тільки для 0,49% вузлових пар в порівнянні з OLSR. Хоча з коефіцієнтом 20% і тим же радіусом, результати все ще відмінні лише з 1,33% пар вузлів без шляху.

Таблиця 3.4 Довжина шляхів SU-OLSR (Критерій II + Варіант I) проти OLSR

Δ	190 *m*	230 *m*	250 *m*	250 *m*
Коефіцієнт	0.25	0.25	0.25	0.20
0	0.5937	0.8767	0.9312	0.8808
1	0.1012	0.0705	0.0493	0.0765
2	0.0430	0.0175	0.0104	0.0196
3	0.0226	0.0059	0.0027	0.0060
4	0.0115	0.0025	0.0001	0.0022

Продовження таблиці 3.4

≥ 5	0.0161	0.0018	0.0005	0.0015
∞	0.2120	0.0256	0.0049	0.0133

Випадок II варіанту:

Для того, щоб побачити, чи може протокол працювати краще у випадку Критерію I, ми зменшимо обмеження. Таким чином, протокол SU-OLSR може використовувати MPR, визнаний безпечним певними вузлами, для обчислення його шляхів між парами вузлів.

Запропоновано три альтернативи:

Варіант II-a: MPR, оголошені безпечними всіма вузлами або певними вузлами, використовуються без відмінностей.

Варіант II-b: MPR, визнані безпечними всіма вузлами, є кращими, ніж ті, що визнані безпечними деякими вузлами.

Варіант II-c: посилання, яке визнано небезпечним деякими вузлами, може бути використано лише для останнього переходу, щоб завершити шлях до місця призначення.

Обидва варіанти II-a та II-b можуть бути реалізовані шляхом співставлення різних ваг з краями E_{MPRSel}. Таким чином, ми отримаємо оцінений граф. На Рис. 3.5 показані пов'язані ваги для цих двох варіантів. На цьому малюнку, вузли A і B розглядають вузол M як MPR безпечний, тоді як вузол C оголошує його небезпечним.

У випадку варіанту II-a вага w = 1 пов'язана з ребрами, вершина яких є MPR, що визнаний безпечним всіма або деякими вузлами (див. Рис. 3.5- (a)). В той час як у випадку Варіант II-b ваги w = 1 і w = n пов'язані відповідно з ребрами, вершина яких є MPR, що визнаний безпечний всіма вузлами і MPR, що визнаний безпечними певними вузлами (див. Рис. 3.5 - (б)). Параметр n представляє тут кількість вузлів у мережі. В обох випадках, таким чином, можна використовувати оголошений безпечний MPR вузлом для досягнення цього вузла, незалежно від оцінки того, що інші вузли роблять цей MPR.

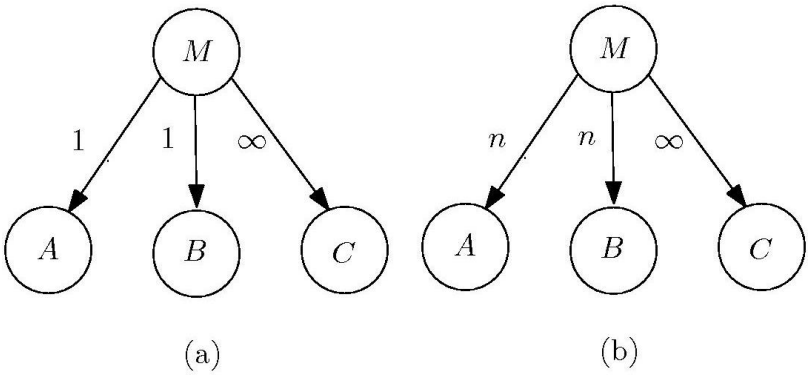

Рисунок 3.5 Зв'язані ваги для варіанту II-a та II-b

По конструкції довжина найкоротших шляхів менше n у випадку варіанту II-a. В іншому випадку довжина найкоротших шляхів має вигляд a * n + b, де a - кількість стрибків, що проходять повз ребер, вершини яких MPR визнані небезпечними певними вузлами; b - кількість стрибків, що проходять через ребра, вершини яких MPR визнані безпечними всіма вузлами мережі.

Таблиця 3.5 порівнює протокол OLSR з варіантом II-a протоколу SU-OLSR, де MPR, визнані захищеними всіма вузлами або певними вузлами, використовуються без відмінностей. Відзначено, що SU-OLSR забезпечує хорошу продуктивність у порівнянні зі звичайним протоколом OLSR. Наприклад, у випадку SU-OLSR з радіусом зв'язку 250 м, більше 79,87% пар вузлів не бачать зміни довжини їх найкоротшого шляху. Відзначимо також, що в цьому випадку 17,84% вузлів бачать довжину свого найкоротшого шляху збільшується на один крок і на 1,47% від двох кроків.

При цьому всього 0,46% пар вузлів не можуть знайти дійсний шлях (вузли відключені від мережі). Продуктивність у футлярі радіусу 290m ідеально. Найкоротший шлях лише 7,9% пар вузлів був збільшений на один крок.

Таблиця 3.5 Довжина шляхів SU-OLSR (Критерій I + Варіант II-a) проти OLSR

Δ	190 *m*	230 *m*	250 *m*	290 *m*
0	0.4456	0.7065	0.7987	0.9192
1	0.1970	0.2275	0.1784	0.0795
2	0.1009	0.0425	0.0147	0.0007
3	0.0490	0.0096	0.0023	0.00005
4	0.0278	0.0038	0.0008	–
5	0.0161	0.0016	0.0003	–
6	0.0096	0.0005	0.00004	–
7	0.0063	0.0002	0.00001	–
≥ 8	0.0131	0.00006	–	–
∞	0.1346	0.0077	0.0046	0.0005

У випадку Варіант II-b, MPR, визнані безпечними всіма вузлами порівняно з заявленими безпечними, є кращими для деяких вузлів для побудови найкоротшого шляху між вузлами. За допомогою цього варіанту, замість створення більш коротких шляхів зі змішаними MPR, протокол SU-OLSR надає перевагу шляхам, які не проходять через оголошені небезпечні MPR, навіть якщо його шляхи більше. Таким чином, SU-OLSR вибирає найкоротший шлях, мінімізуючи кількість небезпечних використовуваних MPR.

Таблиця 3.6 Довжина шляху SU-OLSR (Критерій I + Варіант II-b) проти OLSR

Ω	Δ	190 *m*	230 *m*	250 *m*	290 *m*
0	0	0.3128	0.4673	0.5357	0.6773
0	1	0.0210	0.0413	0.0486	0.0582
0	2	0.0053	0.0166	0.0188	0.0257
0	3	0.0016	0.0074	0.0074	0.0104
0	4	0.0009	0.0034	0.0031	0.0041

Продовження таблиці 3.6

0	≥ 5	0.0002	0.0031	0.0021	0.0027
1	0	0.0891	0.1424	0.1545	0.1377
1	1	0.0554	0.0796	0.0769	0.0414
1	2	0.0155	0.0230	0.0237	0.0109
1	≥ 3	0.0072	0.0161	0.0168	0.0056
2	0	0.0232	0.0342	0.0296	0.0128
2	1	0.0658	0.0630	0.0411	0.0099
2	2	0.0283	0.0201	0.0114	0.0011
2	≥ 3	0.0191	0.0152	0.0079	0.0005
≥ 3	–	0.2205	0.0595	0.0178	0.0011
–	∞	0.1346	0.0077	0.0046	0.0005

Таблиця 3.6 показує різницю в довжині шляху між OLSR і SU-OLSR з використанням цієї опції. Перший стовпець представляє число незабезпечених MPR, використовуваних для побудови найкоротшого шляху. Зверніть увагу, що при використанні безпечного MPR ($\Omega = 0$) отримані результати такі ж, як і у випадку Варіанта I (див. Табл. 3.3). Також можна зазначити, що останній рядок ($\Delta = \infty$) Таблиці 3.5 і Таблиці 3.6 є ідентичними. Дійсно, зв'язність графа та існування шляхів між вузлами не залежать від вибору Варіанта II-a або Варіанта II-b. Єдине, що змінюється між двома варіантами - це довжина шляхів між вузлами.

Ефективність протоколу SU-OLSR дуже хороша. Для побудови найкоротших шляхів для кожного вузла з радіусом зв'язку 250 м, 61,57% пар вузлів використовують тільки безпечні MPR для, 27,19% вузлів використовують один незахищений MPR, 9% пар вузлів використовують два Незабезпечені MPRs, 1,78% пар вузлів використовують більше трьох незабезпечених MPR, і в кінцевому рахунку тільки пари вузлів не підключені.

3.6 Результати моделювання

- Кількість MPR

Мобільність і щільність мережі мають безпосередній вплив на алгоритми вибору MPR. Таблиці 3.7 і 3.8 показують вплив цих параметрів на кількість MPR, вибраних для сценаріїв мобільності, при 1,4 м / с і 10 м / с. Розрахунок MPR проводиться кожну секунду моделювання. Ці результати є середніми з усіх моделювань.

В обох таблицях кількість MPR є майже однаковою для обох протоколів з невеликою перевагою для OLSR, яка вибирає менше MPR. Наприклад, для радіусу зв'язку 230 м, середнє значення MPR, обраних у випадку сценаріїв мобільності зі швидкістю 1,4 м / с, становить 81,55 MPR для протоколу SU-OLSR. Для тих самих сценаріїв середній показник для протоколу OLSR становить 76,27 MPR.

Таблиця 3.7 Кількість MPR у випадку максимальної рухливості 1,4 м/с

Радіус зв'язку		190 *m*	230 *m*	250 *m*	290 *m*
SU-OLSR	μ	80.67	81.55	80.78	77.30
	σ^2	2.65	2.45	0.94	2.39
OLSR	μ	78.97	76.27	77.04	73.70
	σ^2	1.38	5.33	0.79	2.99

Для сценаріїв високої мобільності обидва протоколи вибирають більше MPR. Якщо взяти сценарії з максимальною швидкістю 10 м / с, то для радіуса зв'язку 230 м у протоколі SU-OLSR вибирається в середньому 87,91 MPR. З іншого боку, OLSR вибирає в середньому лише 85,79 MPR. Таке велике число MPR пояснюється нестабільністю мережі на цій швидкості.

Таблиця 3.8 Кількість MPR в разі максимальної рухливості 10 м / с

Радіус зв'язку		190 *m*	230 *m*	250 *m*	290 *m*
SU-OLSR	μ	87.91	87.29	85.44	77.30
	σ^2	0.53	1.14	1.62	2.39
OLSR	μ	85.79	84.84	83.84	73.70
	σ^2	1.67	1.32	2.23	2.99

Щоб правильно вивчити поведінку двох алгоритмів вибору MPR, розраховується кожна секунда різниці між числами MPR, вибраними двома протоколами. Ці розрахунки виконуються з однаковим сценарієм мобільності. Рис. 3.6 показує цю різницю для сценарію мобільності 1,4 м / с. Відзначимо, що різниця між кількістю MPR для двох протоколів постійно змінюється.

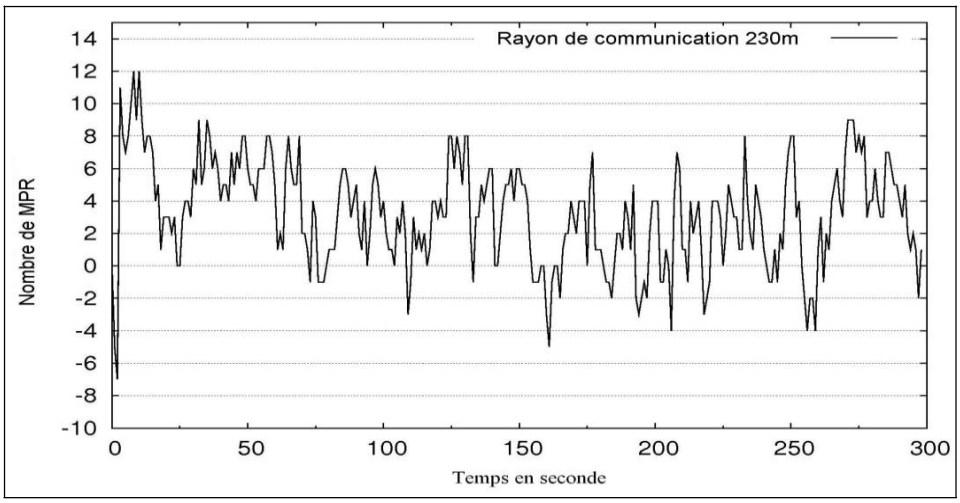

Рисунок 3.6 Різниця MPR, обрана між двома протоколами (швидкість 1,4 м / с max)

Те ж саме стосується сценарію мобільності в 10 м / с (див. Рис. 3.7). Слід зазначити, що на цій швидкості мережа нестабільна, що пояснює великі флуктуації на графіку в порівнянні з графіком рисунка 3.6

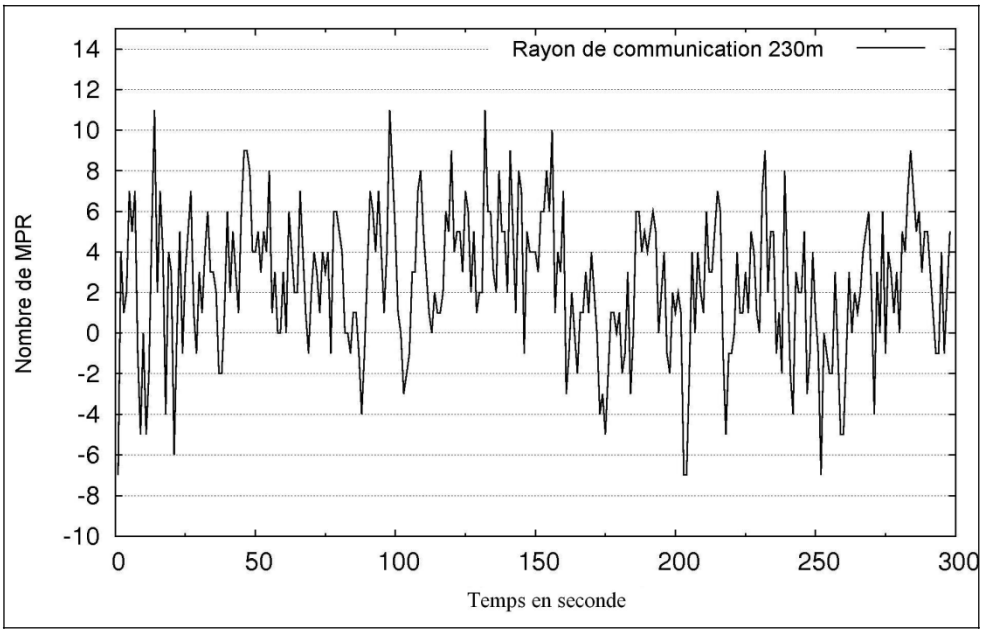

Рисунок 3.7 Різниця MPR, обрана між двома протоколами (швидкість 10 м/с max)

- Відсоток поставлених пакетів

На Рисунку 3.8 показаний відсоток доставлених пакетів порівняно із середньою швидкістю вузла з радіусом зв'язку 230 м з використанням протоколу OLSR і SU-OLSR. Коли вузли стаціонарні (швидкість = 0 м / с), зв'язок між вузлами практично не містить пакетів для протоколів OLSR і SU-OLSR. У цьому статичному випадку протокол OLSR має невелику перевагу, оскільки 99,88% доставлених пакетів проти 99,29% для SU-OLSR.

З іншого боку, коли швидкість вузлів збільшується, продуктивність обох протоколів погіршується. Така деградація продуктивності зумовлена швидкістю, з якою обидва протоколи потребують оновлення таблиць маршрутизації та визначення MPR. У середовищі з високою мобільністю зв'язки між вузлами дуже швидко змінюються і зв'язки між вузлами існують протягом дуже коротких періодів часу. З іншого боку, для мереж з низькою мобільністю або нульовою мобільністю зв'язки існують протягом дуже тривалого періоду часу, що сприяє коректному передачі трафіку CBR до місця призначення.

Однак, до швидкості рухливості 5 м / с, два протоколи показують однакову поведінку. З іншого боку, від 10 м / с протокол SU-OLSR має переваги порівняно з OLSR. PDR SU-OLSR становить 38,46% проти 37,41% для OLSR при швидкості 20 м / с. Ці результати, отримані для двох протоколів, узгоджуються з OLSR

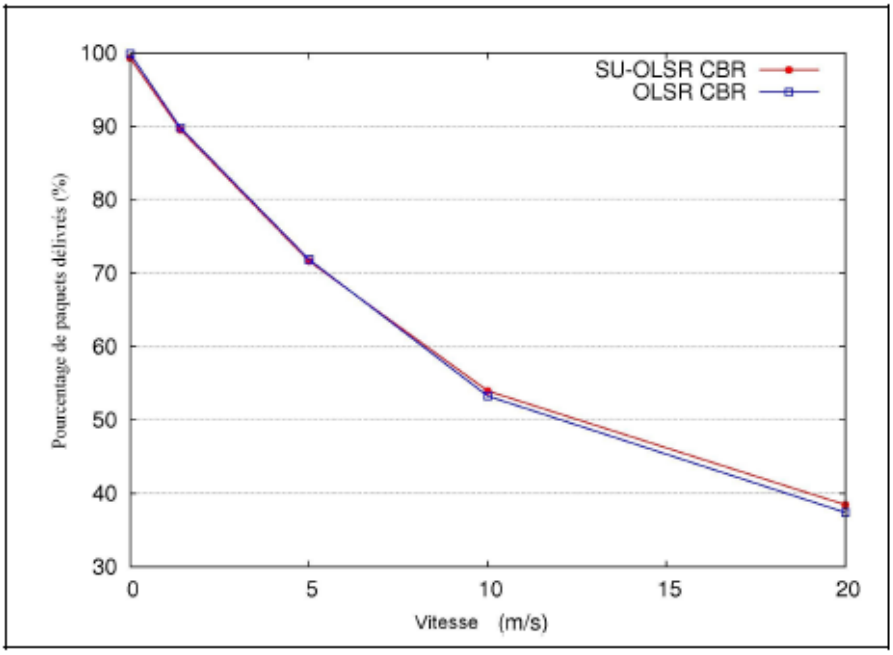

Рисунок 3.8 Відсоток пакетів, що доставляються PDR для обох протоколів

- Наскрізна затримка

Наскрізна затримка IP-пакета в мережах - це сума затримок, що вводяться проміжними вузлами між джерелом і місцем призначення. Це залежить від часу обробки в проміжному вузлі, затримки черги, затримки при відправці на фізичному носії і затримки поширення відповідно до відстані. На Рисунку 3.9 показано кінцеву затримку щодо швидкості вузлів мережі з радіусом зв'язку 230 м. Відзначимо, що ця затримка зростає зі швидкістю. Для мережі з високою мобільністю (20 м / с) ця затримка є максимальною. Ця деградація може бути пояснена тим, що на цій швидкості MPR можуть рухатися далеко і з вузлів, які обрали їх як MPR, і це може відбутися дуже

швидко. Це призводить до перерв у зв'язках між джерелом трафіку Constant Bit Rat (CBR) і місцем призначення.

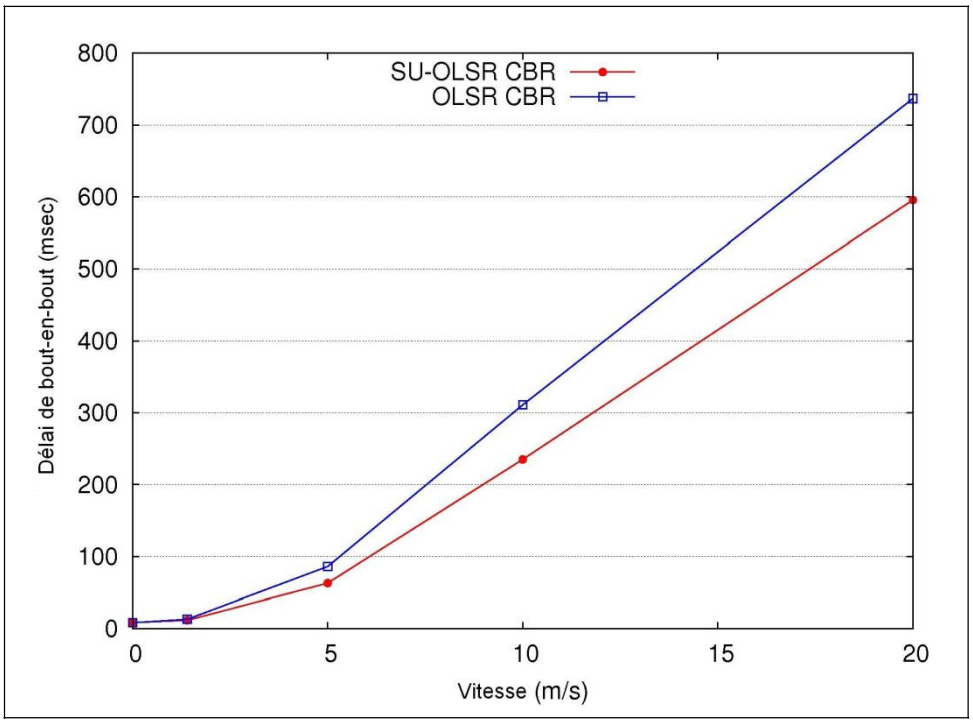

Рисунок 3.9 Затримка на обох протоколах

З іншого боку, додаткову затримку вводять через процес відбору PRM для заміни відключених MPR і пошуку нових шляхів до пункту призначення. Це безпосередньо впливає на продуктивність протоколів OLSR і SU-OLSR.

Зазначимо, що протокол SU-OLSR використовує переваги над OLSR для мереж високої мобільності. Більша кількість MPR, відібраних SU-OLSR на цій швидкості мобільності порівняно з OLSR, пояснює цю незначну перевагу в кінцевій затримці для SU-OLSR. Якщо розглядати фіксований випадок (0 м / с), протокол OLSR має невелику перевагу в затримці з 8,3 мс проти 8,5 мс для SU-OLSR. Те ж саме стосується максимальної затримки (див. Рис. 3.10). Це підтверджує результати, отримані в нашому статичному моделюванні (див. Таблиця 3.5). Зазначимо, що обидва протоколи отримують однакову довжину шляху для 70,5% пар вершин. Це пояснює цю незначну різницю у затримці між двома протоколами SU-OLSR і OLSR

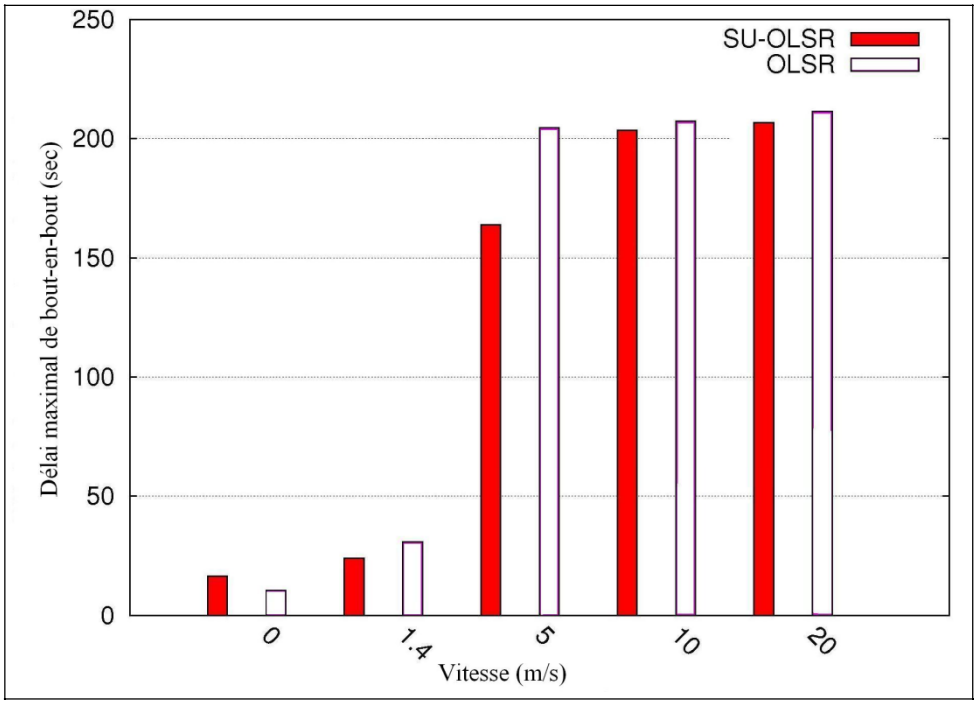

Рисунок 3.10 Максимальна затримка з обох протоколів

Рис. 3.11 показує кількість повідомлень, що передаються під час моделювання, як функції швидкості руху. Ми відзначаємо деградацію продуктивності двох протоколів у сценаріях високої мобільності, але з невеликим прогресом для SU-OLSR.

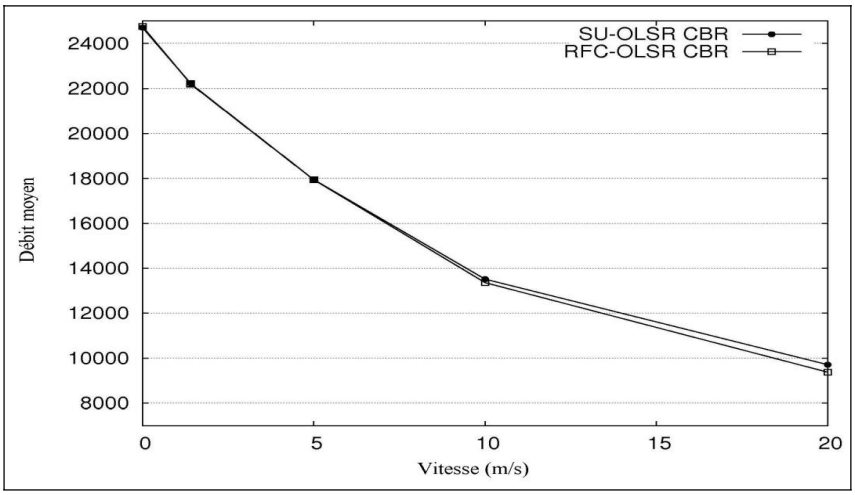

Рисунок 3.11 Кількість доставлених повідомлень

3.7 Висновки з розділу 3

Існує проблема, коли зловмисний вузол змушує своїх сусідів вибирати його як MPR. Для цього достатньо, щоб зловмисний вузол оголосив, що він має прямий зв'язок з віддаленим або неіснуючим вузлом у мережі. Після вибору MPR, цей вузол матиме перевагу в мережі, оскільки він може змінювати, змінювати або відхиляти трафік, який проходить через нього. Це становить небезпеку для цілісності, конфіденційності та доступності комунікацій.

Щоб подолати це обмеження протоколу OLSR, існує SU-OLSR. SU-OLSR запобігає вибору будь-якого зловмисного вузла, який представляє певну підозрілу поведінку, як MPR. Ми визначили два критерії відхилення зловмисного вузла. Перший критерій - коли вузол охоплює ізольований вузол. Другий - коли вузол заявляє, що він охоплює більше, ніж попередньо визначену частину своїх сусідів. Таким чином, вузол, який має один з цих критеріїв, буде оголошений підозрілим і буде автоматично відхилений від фази вибору MPR за допомогою SU-OLSR. Зі свого боку, розрахунок шляху здійснюється за чотирма варіантами. Алгоритм Дейкстри або використовує MPR, оголошений безпечним всіма вузлами, або використовує без відмінності MPR, визнаний безпечним всіма або певними вузлами, або переважно використовує MPR, визнаний безпечним всіма вузлами, або, нарешті, не використовує оголошену посилання. небезпечні деякими вузлами останнього стрибка, щоб завершити шлях до пункту призначення.

При такому підході деякі законні вузли, на жаль, можуть мати один з цих критеріїв. Це виключає їх з фази вибору MPR, що може мати вплив на підключення до мережі. Тому ми спробували, як другу фазу, експериментально вивчити наш підхід і довести, що новий протокол SU-OLSR показує продуктивність, порівнянну з класичним протоколом OLSR, незважаючи на те, що SU-OLSR є більш вибірковим.

Ми розпочали нашу експериментальну оцінку з розробкою програми C для моделювання двох протоколів SU-OLSR та OLSR в середовищі без мобільності. Ці моделювання дозволили нам побачити продуктивність SU-OLSR та OLSR відносно кількості обраних MPR та довжини найкоротшого шляху між вузлом-джерелом та кінцевим вузлом. Ці обнадійливі результати показали, що показники цих двох протоколів дуже близькі.

Вище було сказано, що зловмисний M вузол може брехати про свій справжній статус. Тому, якщо такий вузол заявляє, що він був обраний як довірений MPR вузлом X, то цей вузол отримає TC повідомлення, в якому побачить, що небезпечний вузол говорить про те, що він був вибраний як MPR нашим вузлом X. В такому випадку, вузол повинен застосувати певний механізм щоб денонсувати шкідливий вузол від інших вузлів мережі. На жаль, такий механізм ще не був застосований, тому потрібно запропонувати та перевірити роботу такого механізму.

ВИСНОВКИ

OLSR є одним із найсучасніших протоколів маршрутизації. Даний протокол розроблений для мобільних спеціальних мереж. Він функціонує як проактивний протокол, керований таблицями. Тобто він користується популярністю через свою змогу передавати HELLO та TC повідомлення, які дозволяють всім вузлам мережі мати інформацію про сусідні вузли.

В першому розділі було розглянуто саму структуру основного протоколу OLSR та визначено його переваги та недоліки. Завдяки цьому, у другому розділі було систематизовано декілька варантів модифікацій OLSR. Кожна модифікація усуває деякі недоліки протоколу OLSR.

OLSR не розглядає такі параметри, як енергетичний рівень вузлів та довжину зв'язків у обробці маршруту. Штучна імунна система (AIS) використовується для підвищення ефективності протоколу маршрутизації OLSR. Запропонований алгоритм, що називається AIS-OLSR, враховує кількість переходів, залишкову енергію в проміжних вузлах та відстань між вузлами, яка реалізується за допомогою негативного відбору та алгоритмів ClonalG AIS. AIS-OLSR перевершує OLSR з точки зору коефіцієнту передачі пакетів, пропускної спроможності, кінцевої затримки та терміну служби.

Інформація про стан для маршрутизації в протоколі OLSR є по суті неточною. Маршрутизація QoS може сильно постраждати через декілька факторів, включаючи радіоперешкоди на доступній пропускній здатності та неефективне затоплення інформації до сусідніх вузлів. В результаті продуктивність мережі істотно погіршується. Порівняльне дослідження показує, що, незважаючи на накладні витрати, пов'язані з управлінням QoS, цей варіант протоколу кращий, ніж класичний протокол OLSR, з точки зору QoS та ефективного використання енергії.

У порівнянні з протоколом маршрутизації OLSR, MP-OLSR забезпечує більш коротку затримку передачі завдяки збору інформації топології

заздалегідь. Крім того, він може виявити кілька шляхів більш ефективно, без особливих додаткових витрат.

Вибір MPR є однією з основних задач протоколу OLSR. Якщо в MPR вибрати один із шкідливих вузлів це може призвести до зміни напрямку трафіку або взагалі до втрати інформації, що передається.

SU-OLSR запобігає вибору будь-якого зловмисного вузла, який представляє певну підозрілу поведінку, як MPR. Підозрілим вузол вважається, якщо він охоплює один або кілька ізольованих вузлів в $N_2(S)$. Такий вузол буде автоматично відхилений від фази вибору MPR за допомогою SU-OLSR.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Abdellaoui R. SU-OLSR une nouvelle solution pour la securite du protocole OLSR. / Rachid Abdellaoui. // Ecole de technologie soperieure universite du Quebec. – 2009.

2. Optimized Link State Routing Protocol / [T. Clausen, P. Jacquet, C. Adjih та ін.]. // Network Working Group. – 2003. – С. 75.

3. Jubin J. The DARPA Packet Radio Network Protocols / J. Jubin, D. Tornow. – 1987.

4. Freebersyser, J. A., et B. Leiner. 2001. « A DoD perspective on mobile Ad hoc networks ». In Ad hoc networking; C.E Perkins Ed. C. 29-51. Addison-Wesley Longman Publishing Co., Inc.

5. Fifer, W. C., et F. J. Bruno. 1987. « The low-cost packet radio ». Proceedings of the IEEE, vol. 75, № 1, C. 33-42.

6. Multipath Optimized Link State Routing for Mobile adhoc Networks / Y.Jiazi, A. Hassiba, D. Sylvain, P. Benoît. – 2010. – С. 17.

7. Кирьянов А. Методы исследования переходных характеристик протокола OLSR при включений/выключении узла сети. / А. Кирьянов, А. Сафонов, Е. Хоров. – С. 29

8. P. Jacquet, P. Minet, P. Muhlethaler, N. Rivierre. Increasing reliability in cable free radio LANs: Low level forwarding in HIPERLAN. Wireless Personal Communications. – 1996.

9. F. Sarkohaki, R. Fotohi, V. Ashrafian. An Efficient Routing Protocol in Mobile Ad-hoc Networks by using Artificial Immune System. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 4, 2017

10. J. H¨arri, F. Filali, and C. Bonnet, “Kinetic multipoint relaying: improvements using mobility predictions,” in Active and Programmable Networks. Springer, pp. 224–229, 2009.

11. S. Banik, B. Roy, P. Dey. QoS Routing using OLSR with Optimization for Flooding. – C. 4.

12. J. Wen. Multiple Path Optimized Link State Routing (MP-OLSR). Multimedia and Data Management – 2013. – C. 46

13. Mans, B., et N. Shrestha. 2004. «Performance Evaluation of Approximation Algorithms for Multipoint Relay Selection». In Proceedings of the 3rd Annual Mediterranean Ad-Hoc Workshop Med-Hoc-Net. p. 480-491.

14. Matousek, J. , J. Nesetril et D. Hachez. Introduction Aux Mathématiques Discrètes. Springer. – 2004.

15. Adjih, C., P. Jacquet et L. Viennot. 2002. Computing Connected Dominated Sets with Multipoint Relays. Coll. « INRIA Technical report RR-4597 ». INRIA

16. Wu, J., Lou Wei et F. Dai. « Extended multipoint relays to determine connected dominating sets in MANETs ». In Proceedings of the IEEE Computers vol. 55 - № 3. – 2006. – C. 334-347.

17. Badis, H., A. Munaretto, K. Al Aghal et G. Pujolle. 2004. « Optimal path selection in a link state QoS routing protocol ». In In Proceedings of the 59th IEEE Vehicular Technology Conference VTC 2004-Spring. Vol. 5, p. 2570-2574.

18. Ge, Y., T. Kunz et L. Lamont. 2003. « Quality of service routing in ad-hoc networks using OLSR ». In In Proceedings of the 36th Annual Hawaii International Conference onSystem Sciences p. 9.

19. J. Harri, F. Filali, C. Bonnet. Kinetic multipoint relaying: improvements using mobility predictions. – 2009. – C. 224–229.

20. Penrose, M. 2003. Random Geometric Graphs. Coll. « Oxford Studies in Probability ». Oxford University Press.

21. Penrose, M. 1999. « On k-connectivity for a geometric random graph ». Random Structures and Algorithms, vol. 15, no 2, p. 145-164.

22. M. Barbeau, M., et E. Kranakis. 2007. Principles of Ad Hoc Networking. Wiley.